EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S AMENDED NOTICE OF SERVING SUBPOENA FOR VIDEOTAPED DEPOSITION OF SHIVA AYYADURAI**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Shiva Ayyadurai, 69 Snake Hill Road, Belmont, MA 02478-1505 A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 19, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 19, 2023 a true and accurate copy of the foregoing was served via email to the following attorneys of record for Plaintiffs:

ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402

Christopher K. Larus	CLarus@robinskaplan.com
William E. Manske	WManske@robinskaplan.com
Emily J. Tremblay	ETremblay@robinskaplan.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

J. Erik Connolly	EConnolly@beneschlaw.com
Nicole E. Wrigley	NWrigley@beneschlaw.com
Michael E. Bloom	MBloom@beneschlaw.com
Laura A. Seferian	LSeferian@beneschlaw.com
Julie M. Loftus	JLoftus@beneschlaw.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
200 Public Square, Suite 2300
Cleveland, OH 44114

Alyssa A. Moscarino	AMoscarino@beneschlaw.com
James R. Bedell	JBedell@beneschlaw.com

DATED: September 19, 2023 By: *Andrew D. Parker*

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al.
Plaintiff
v.
Michael J. Lindell and My Pillow, Inc., et. al.
Defendant

Civil Action No. 21-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Shiva Ayyadurai
69 Snake Hill Road, Belmont, MA 02478-1505
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about these matters: **See, attached Exhibit A**

Place:	Date and Time:
Veritext - (Conf Suites) 101 Arch Street, Suite 650, Boston, MA 02100	10/06/2023 9:00 am EDT

The deposition will be recorded by this method: stenographic and videotaped

❒ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: September 19, 2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

s/ Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Defendants' Michael J. Lindell and My Pillow, Inc., et al., who issues or requests this subpoena, are:

Andrew Parker, 123 North Third Street, Suite 888, Minneapolis MN 55401; parker@parkerdk.com; 612-355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 21-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S NOTICE OF SERVING SUBPOENA FOR VIDEOTAPED DEPOSITION OF HARRI HURSTI**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Harri Hursti, 274 Valley Road Apt. 2, Cos Cob, CT 06807. A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 19, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 19, 2023 a true and accurate copy of the foregoing was served via email to the following attorneys of record for Plaintiffs:

ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402

Christopher K. Larus	CLarus@robinskaplan.com
William E. Manske	WManske@robinskaplan.com
Emily J. Tremblay	ETremblay@robinskaplan.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

J. Erik Connolly	EConnolly@beneschlaw.com
Nicole E. Wrigley	NWrigley@beneschlaw.com
Michael E. Bloom	MBloom@beneschlaw.com
Laura A. Seferian	LSeferian@beneschlaw.com
Julie M. Loftus	JLoftus@beneschlaw.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
200 Public Square, Suite 2300
Cleveland, OH 44114

Alyssa A. Moscarino	AMoscarino@beneschlaw.com
James R. Bedell	JBedell@beneschlaw.com

DATED: September 19, 2023 By: *Andrew D. Parker*

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al.
Plaintiff
v.
Michael J. Lindell and My Pillow, Inc., et. al.
Defendant

Civil Action No. 21-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: **Harri Hursti**
274 Valley Road Apt. 2, Cos Cob, CT 06807
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about t these matters: **See, attached Exhibit A.**

Place:	Date and Time:
Regus - 500 West Putnam Avenue Suite 400 Greenwich, CT 06830	October 9 2023 at 9:00 a.m. EDT

The deposition will be recorded by this method: stenographic and videotaped

❒ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 09/19/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

s/ Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* **Defendants' Michael J. Lindell and My Pillow, Inc., et al.**, who issues or requests this subpoena, are:

Andrew Parker, 123 N. 3rd Street, Suite 888, Minneapolis MN 55401, parker@parkerdk.com, 612-355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 21-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S NOTICE OF SERVING SUBPOENA FOR DEPOSITION OF CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Cybersecurity & Infrastructure Security Agency c/o Office of the Chief Counsel, 1616 Fort Myer Drive, Arlington, VA 22209, cisa.occ@cisa.dhs.gov. A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 22, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp. et al. *Plaintiff* v. Michael J. Lindell et al. *Defendant*	)	Civil Action No. 22-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Cybersecurity & Infrastructure Security Agency
c/o Office of the Chief Counsel, 1616 Fort Myer Drive, Arlington, VA 22209, cisa.occ@cisa.dhs.gov
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about these matters:

Place:	Date and Time:
Regus 4250 North Fairfax Drive, Suite 600 Arlington, Virginia 22203	10/13/2023 9:00 am

The deposition will be recorded by this method: Audio/video and stenographic transcription

☐ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 09/22/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* My Pillow, Inc. and Michael Lindell, who issues or requests this subpoena, are:

Andrew D. Parker, 888 Colwell Building, 123 N. 3rd St., Minneapolis, MN 55401, parker@parkerdk.com, (612) 355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 22-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____ _____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT 1

Federal Rule of Civil Procedure 30(b)(6) Notice

This subpoena is issued pursuant to Federal Rule of Civil Procedure 30(b)(6) naming as the deponent the United States Cybersecurity & Infrastructure Security Agency ("CISA"), a governmental agency.

Pursuant to Rule 30(b)(6), as recipient of this subpoena, CISA must do both of the following:

- CISA must "designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on its behalf; and it may set out the matters on which each person designated will testify." The persons designated must "testify about information known or reasonably available to the organization."
- CISA "must confer in good faith about the matters for examination" with the party serving the subpoena.

Counsel for the serving party will confer with counsel for CISA about the matters for examination. The matters for examination in the deposition are as follows:

1. The November 12, 2020 *Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees* ("Joint Statement," attached as Exhibit 2), specifically:

    a. Authentication of a copy of the Joint Statement
    b. The process that was followed to establish the factual bases for the Joint Statement
    c. The basis for the Joint Statement's assertion that "The November 3rd election was the most secure in American history."

d. The process that was followed to determine whether "The November 3rd election was the most secure in American history."
e. The basis for the Joint Statement's assertion that "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised."
f. The process that was followed to determine whether there was any "evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised."
g. Whether any elected official had any involvement in the process that resulted in the Joint Statement, and if so, the identity of the elected officials and the nature of their involvement
h. Whether any person outside of the signatories of the Joint Statement had any involvement in the process that resulted in the Joint Statement, and if so, the identity of those persons and the nature of their involvement
i. Confirmation that CISA has no file of information supporting the assertion in the Joint Statement that "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised," per CISA's response to the previous document subpoena issued in the above-captioned case.

2. The June 3, 2022 *ICS Advisory (ICSA-22-154-01) Vulnerabilities Affecting Dominion Voting Systems ImageCast X* (attached as Exhibit 3) specifically,
   a. Authentication of a copy of ICSA-22-154-01
   b. The basis for the assertion in ICSA-22-154-01 that CISA has "no evidence that these vulnerabilities [identified in ICSA-22-154-01] have been exploited in any elections."
   c. The process that was followed to determine whether there was any evidence that a vulnerability identified in ICSA-22-154-01 has been exploited in any election.
   d. Confirmation that CISA has no file of information supporting the assertion in ICSA-ss-154-01 that CISA has "no evidence that these vulnerabilities [identified in ICSA-22-154-01] have been exploited in any elections," per CISA's response to the previous document subpoena issued in the above-captioned case.

3. CISA's knowledge of any actual, suspected, or reported instance of Unauthorized Access to Electronic Election Equipment located in the United States that occurred between October 1, 2020 and November 30, 2020, specifically:
    a. What information or allegation CISA received
    b. What investigation CISA performed in response to any such information or allegation
    c. What facts CISA discovered as the result of any such investigation

4. CISA's knowledge of any cybersecurity breach that affected any vote tally in a U.S. election

5. CISA's knowledge concerning whether any U.S. city, county, or local jurisdiction's Election Management System or optical ballot scanner(s) were connected to the Internet, or could be connected to the Internet, in October or November 2020.

6. CISA's response to the previous document subpoena issued in the above-captioned case, attached as Exhibit 4.

7. CISA's Election Infrastructure Insider Threat Mitigation Guide (Exhibit 5, obtained from https://www.cisa.gov/resources-tools/resources/election-infrastructure-insider-threat-mitigation-guide on September 22, 2023), specifically

    a. Authentication of the document as a CISA publication
    b. The purpose of the document and the general sources of its information
    c. The scope of "insider threats" as discussed in the document
    d. The scope of "Cybersecurity Incidents" referenced in the document

8. CISA's July 28, 2020 "Election Infrastructure Cyber Risk Assessment (Exhibit 6, obtained from https://www.cisa.gov/resources-tools/resources/election-infrastructure-cyber-risk-assessment on September 22, 2023), specifically

    a. Authentication of the document as a CISA publication
    b. Publication of the document on July 28, 2020
    c. The purpose of the document and the general sources of its information

d. The "key finding" that "Compromises to the integrity . . . vote aggregation systems . . . present particular risk to the ability of jurisdictions to conduct elections."
e. The "key finding" that "However, even jurisdictions that implement cybersecurity best practices are potentially vulnerable to cyber attack by sophisticated cyber actors, such as nation-state actors."

"Electronic Election Equipment" means any electronic device used, by or on behalf of a state or local government authority, in the administration of vote casting, collecting, counting or tabulating tasks during a public election.

"Unauthorized Access" means the viewing, modification, or deletion of electronically stored data by a person not authorized, by the owner of the electronic equipment on which the data was stored, to perform this activity.

EXHIBIT 2

PRESS RELEASE

Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees

Released: November 12, 2020

Revised: November 12, 2020

RELATED TOPICS: ELECTION SECURITY </topics/election-security>

WASHINGTON – The members of Election Infrastructure Government Coordinating Council (GCC) Executive Committee – Cybersecurity and Infrastructure Security Agency (CISA) Assistant Director Bob Kolasky, U.S. Election Assistance Commission Chair Benjamin Hovland, National Association of Secretaries of State (NASS) President Maggie Toulouse Oliver, National Association of State Election Directors (NASED) President Lori Augino, and Escambia County (Florida) Supervisor of Elections David Stafford – and the members of the Election Infrastructure Sector

Coordinating Council (SCC) – Chair Brian Hancock (Unisyn Voting Solutions), Vice Chair Sam Derheimer (Hart InterCivic), Chris Wlaschin (Election Systems & Software), Ericka Haas (Electronic Registration Information Center), and Maria Bianchi (Democracy Works) - released the following statement:

“The November 3rd election was the most secure in American history. Right now, across the country, election officials are reviewing and double checking the entire election process prior to finalizing the result.

“When states have close elections, many will recount ballots. All of the states with close results in the 2020 presidential race have paper records of each vote, allowing the ability to go back and count each ballot if necessary. This is an added benefit for security and resilience. This process allows for the identification and correction of any mistakes or errors. **There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised.**

“Other security measures like pre-election testing, state certification of voting equipment, and the U.S. Election Assistance Commission’s (EAC) certification of voting equipment help to build additional confidence in the voting systems used in 2020.

“While we know there are many unfounded claims and opportunities for misinformation about the process of our elections, we can assure you we have the utmost confidence in the security and integrity of our elections, and you should too. When you have questions, turn to elections officials as trusted voices as they administer elections.”

###

Related Articles

SEP 20, 2023 **PRESS RELEASE**

CISA, NFL, and Local Partners Conduct Cybersecurity Exercise in Preparation for Super Bowl LVIII </news-events/news/cisa-nfl-and-local-partners-conduct-cybersecurity-exercise-preparation-super-bowl-lviii>

SEP 18, 2023 **PRESS RELEASE**

CISA Sponsors Hack the Building 2.0 Hospital Competition </news-events/news/cisa-sponsors-hack-building-20-hospital-competition>

SEP 13, 2023 **PRESS RELEASE**

Readout from CISA's 2023 Third Quarter Cybersecurity Advisory Committee Meeting </news-events/news/readout-cisas-2023-third-quarter-cybersecurity-advisory-committee-meeting>

SEP 12, 2023 **PRESS RELEASE**

CISA Announces Open Source Software Security Roadmap </news-events/news/cisa-announces-open-source-software-security-roadmap>

Return to top

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>

CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility <https://www.dhs.gov/accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

EXHIBIT 3

ICS Advisory (ICSA-22-154-01)

More ICS-CERT Advisories

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

Legal Notice

1. SUMMARY

This advisory identifies vulnerabilities affecting versions of the Dominion Voting Systems Democracy Suite ImageCast X, which is an in-person voting system used to allow voters to mark their ballot. The ImageCast X can be configured to allow a voter to produce a paper record or to record votes electronically. While these vulnerabilities present risks that should be mitigated as soon as possible, CISA has no evidence that these vulnerabilities have been exploited in any elections.

Exploitation of these vulnerabilities would require physical access to individual ImageCast X devices, access to the Election Management System (EMS), or the ability to modify files before they are uploaded to ImageCast X devices. Jurisdictions can prevent and/or detect the exploitation of these vulnerabilities by diligently applying the mitigations recommended in this advisory, including technical, physical, and operational controls that limit unauthorized access or manipulation of voting systems. Many of these mitigations are already typically standard practice in jurisdictions where these devices are in use and can be enhanced to further guard against exploitation of these vulnerabilities.

2. TECHNICAL DETAILS

2.1 AFFECTED PRODUCTS

The following versions of the Dominion Voting Systems ImageCast X software are known to be affected (other versions were not able to be tested):

- ImageCast X firmware based on Android 5.1, as used in Dominion Democracy Suite Voting System Version 5.5-A
- ImageCast X application Versions 5.5.10.30 and 5.5.10.32, as used in Dominion Democracy Suite Voting System Version 5.5-A
  - **NOTE:** After following the vendor's procedure to upgrade the ImageCast X from Version 5.5.10.30 to 5.5.10.32, or after performing other Android administrative actions, the ImageCast X may be left in a configuration that could allow an attacker who can attach an external input device to escalate privileges and/or install malicious code. Instructions to check for and mitigate this condition are available from Dominion Voting Systems.

Any jurisdictions running ImageCast X are encouraged to contact Dominion Voting Systems to understand the vulnerability status of their specific implementation.

2.2 VULNERABILITY OVERVIEW

NOTE: Mitigations to reduce the risk of exploitation of these vulnerabilities can be found in Section 3 of this document.

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

CVE-2022-1739 has been assigned to this vulnerability.

2.2.2 MUTABLE ATTESTATION OR MEASUREMENT REPORTING DATA CWE-1283

The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device.

CVE-2022-1740 has been assigned to this vulnerability.

2.2.3 HIDDEN FUNCTIONALITY CWE-912

The tested version of ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.

CVE-2022-1741 has been assigned to this vulnerability.

2.2.4 IMPROPER PROTECTION OF ALTERNATE PATH CWE-424

The tested version of ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1742 has been assigned to this vulnerability.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

CVE-2022-1743 has been assigned to this vulnerability.

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1744 has been assigned to this vulnerability.

2.2.7 AUTHENTICATION BYPASS BY SPOOFING CWE-290

The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.

CVE-2022-1745 has been assigned to this vulnerability.

2.2.8 INCORRECT PRIVILEGE ASSIGNMENT CWE-266

The authentication mechanism used by poll workers to administer voting using the tested version of ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.

CVE-2022-1746 has been assigned to this vulnerability.

2.2.9 ORIGIN VALIDATION ERROR CWE-346

The authentication mechanism used by voters to activate a voting session on the tested version of ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.

CVE-2022-1747 has been assigned to this vulnerability.

2.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS** Government Facilities / Election Infrastructure
- **COUNTRIES/AREAS DEPLOYED:** Multiple

- **COMPANY HEADQUARTERS LOCATION:** Denver, Colorado

2.4 RESEARCHER

J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University, reported these vulnerabilities to CISA.

3. MITIGATIONS

CISA recommends election officials continue to take and further enhance defensive measures to reduce the risk of exploitation of these vulnerabilities. Specifically, for each election, election officials should:

- Contact Dominion Voting Systems to determine which software and/or firmware updates need to be applied. Dominion Voting Systems reports to CISA that the above vulnerabilities have been addressed in subsequent software versions.
- Ensure all affected devices are physically protected before, during, and after voting.
- Ensure compliance with chain of custody procedures throughout the election cycle.
- Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.
- Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables.
- Close any background application windows on each ImageCast X device.
- Use read-only media to update software or install files onto ImageCast X devices.
- Use separate, unique passcodes for each poll worker card.
- Ensure all ImageCast X devices are subjected to rigorous pre- and post-election testing.
- Disable the “Unify Tabulator Security Keys” feature on the election management system and ensure new cryptographic keys are used for each election.
- As recommended by Dominion Voting Systems, use the supplemental method to validate hashes on applications, audit log exports, and application exports.
- Encourage voters to verify the human-readable votes on printout.
- Conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records, to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures. These activities are especially crucial to detect attacks where the listed vulnerabilities are exploited such that a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot. (**NOTE:** If states and jurisdictions so choose, the ImageCast X provides the configuration option to produce ballots that do not print barcodes for tabulation.)

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

EXHIBIT 4

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al.,
Plaintiffs
v.
Michael J. Lindell and My Pillow, Inc.
Defendants

Civil Action No. 0:22-cv-00098-WMW-JFD

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: United States Cybersecurity & Infrastructure Security Agency
Office of the Chief Counsel, CISA - NGR STOP 0645, cisa.occ@cisa.dha.gov
(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: See Exhibits A-D attached hereto.

Place:	Date and Time:
Olsen Law, P.C., 1250 Connecticut Ave., NW, Ste. 700, Washington, DC 20036. Alternately, electronic production to parker@parkerdk.com is preferred.	04/28/2023 9:00 am

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 03/29/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Andrew Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Michael J. Lindell and My Pillow, Inc., who issues or requests this subpoena, are:

Andrew Parker, 888 Colwell Building, 123 N. 3rd St., Minneapolis, MN 55401, parker@parkerdk.com, (612) 355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 0:22-cv-00098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Print Save As... Add Attachment Reset

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

DEFINITIONS

1. "Auto-Cast" means a system configuration for a Ballot Marking Device in which the voters are not given the option to verify the printed ballot, either because (1) the paper ballot is dropped into the ballot container without voter review, or (2) the voter preference on the generated paper ballot is marked by an electronic code not interpretable to the voter.

2. "Ballot Marking Device" means a computerized device that displays a digital ballot, and allow voters to make vote selections, then prints a paper record of the voters' choices.

3. "Communication" or "Communications" means a transfer of information in any form, including, without limitation, notes, complaints, diaries, journals, datebooks, reports, calendars, telephone messages, letters, email messages, instant messages (such as, but not limited to, Signal, Cisco Jabber, IBM Sametime, Wickr, ICQ, Kik, BBM, Gchat, iMessage, Telegram, WhatsApp, Slack, and similar types of messages), cell phone text messages (SMS messages, MMS messages or similar communications), voicemail messages, Slack messages or other internal messaging system communications, social media communications or posting on sites including but not limited to Facebook, Twitter, YouTube, Instagram, Gab, or Parler (including any direct messages), website postings, internet chat room postings, lists, correspondence, drawings, designs, telegrams, manuals, summaries or records of personal conversations, logs, minutes or records of meetings, minutes of any other type, transcripts of oral

testimony or statements, affidavits, or summaries of investigations. For avoidance of doubt, the term "Communication" includes internal communications and communications with third parties.

4. "Concerning" means without limitation, containing, reflecting, referring to, alluding to, discussing, relating to, describing, evidencing, supporting, or constituting.

5. "Cybersecurity" means the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (See https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary).

6. "Document" means any printed, written, typed, recorded, transcribed, taped, photographic, or graphic matter, however produced or reproduced, including, but not limited to any letter, correspondence, or communication of any sort; electronic mail, either sent or received; file, print, negative, or photograph; sound or video recording; note, notebook, diary, calendar, minutes, memorandum, contract, agreement, or any amendment thereto; telex, telegram, or cable; summary, report, or record of any telephone conversation, personal conversation, discussion, interview, meeting, conference, investigation, negotiation, act, or activity; projection, work paper or draft; computer output or input; data processing card; opinion or report of any consultant; request, order, invoice, or bill of lading; analysis, diagram, map, index, sketch, drawing, plan, chart, manual, brochure, pamphlet, advertisement, circular, newspaper or magazine clipping; press release; receipt, journal, ledger, schedule, bill, or voucher; financial statement,

statement of account, bank statement, checkbook, check stubs or register, canceled check, deposit slip, charge slip, tax return, or requisition; file, study, graph, or tabulation; and all other writings and recordings of whatever nature, whether signed, unsigned or transcribed, and any other data compilation from which information can be obtained or translated. The term "document" also, shall mean the original and any non-identical original or copy, including those with any marginal note or comment or showing additions, deletions, or substitutions; drafts; attachments to or enclosures with any document; and any other documents referred to or incorporated by reference in the document. The term "document" also specifically includes all electronic documents, electronic Communications, and other "Electronically Stored Information" (whether stored electronically or in the form of a hard-copy, print-out, or otherwise) and all attachments thereto.

7. "Electronic Election Equipment" means any electronic device used, by or on behalf of a state or local government authority in the administration of vote casting, collecting, counting, or tabulating tasks during a public election.

8. "Electronically Stored Information" or "ESI" refers to any portion of data available on a computer or other device capable of storing electronic data. "Electronically Stored Information" includes, but is not limited to, e-mail, spreadsheets, databases, word processing documents, images, presentations, application files, executable files, log files, and all other files present on any type of device capable of storing electronic data. Devices capable of storing electronically stored information include, but are not limited to: servers, desktop computers, portable computers, handheld

computers, flash memory devices, wireless communication devices, pagers, workstations, minicomputers, mainframes, and any other forms of online or offline storage, whether on or off company premises. ESI includes instant messages (such as Signal, Cisco Jabber, IBM Sametime, Wickr, ICQ, Kik, BBM, Gchat, iMessage, Telegram, WhatsApp, Slack, and similar types of messages), cell phone text messages (SMS messages, MMS messages or similar communications), voice mail messages, and similar types of messages. ESI includes any records of such communications or messages, including phone records. ESI includes any social media communication (such as but not limited to Twitter, Facebook, Instagram, YouTube, Parler, Gab, and Periscope), including any direct messages. For any document kept in electronic form, the term "document" includes any metadata associated with the document.

9. "Halderman" means Dr. J. Alex Halderman, who is Professor of Computer Science and Engineering at the University of Michigan as of March 20, 2023 (See https://eecs.engin.umich.edu/people/halderman-j-alex/).

10. "Halderman Report" means the Report and related documents concerning the findings by Halderman referred to in the Notice filed on February 10, 2022 on behalf of CISA, in the United States District Court for the Northern District of Georgia in Curling v. Raffensperger, No. 17-cv-2989, as Document 1314. For ease of reference, the Notice is attached to the foregoing subpoena as Exhibit D.

11. "Joint Statement" means the statement titled "Joint Statement from Elections Infrastructure Government Coordinating Council and The Election Infrastructure Sector Coordinating Executive Committees," dated November 12, 2020,

and published on the CISA website. For ease of reference, a copy of the Joint Statement is attached to the foregoing subpoena as Exhibit B.

12. "Person" means any natural person or any legal entity, including, without limitation, any business or governmental entity or association.

13. The terms "related to," "relates to" or "relating to" mean, refer to, pertain to, reflect, record, describe, allude to, respond to, announce, explain, discuss, show, study, analyze or constitute or be in any other way connected with the matter discussed.

14. "Smartmatic" means Smartmatic USA Corp., Smartmatic International Holding B.V., and/or SGO Corporation Limited.

15. "Unauthorized Access" means the viewing, modification, or deletion of electronically stored data by a person not authorized to perform this activity by the owner of the electronic equipment on which the data was stored.

16. "You," and "Your" and "CISA" mean the United States Cybersecurity & Infrastructure Security Agency and all subunits, divisions, agents, employees, and anyone acting on behalf of the United States Cybersecurity & Infrastructure Security Agency.

17. The present tense includes past and future tenses. The singular includes the plural, and plural includes the singular. "All" means "any and all"; "any" means "any and all." "Including" means "including but not limited to." "And" and "or" encompass "and" and "or." Words in the masculine, feminine or neutral form shall include every gender.

INSTRUCTIONS

1. Each Category herein requires the production of all responsive Documents in the possession, custody, or control of You, or of any of Your respective attorneys, agents and any other persons acting or purporting to act on behalf of any of them, or of any other Person from whom You have the right to obtain Documents, whether in hard-copy or electronic form or in any other form or from any other source, wherever located and however managed, and whether active, in storage, or otherwise.

2. Each Document is to be produced (together with all drafts thereof) in its entirety, without redaction or expurgation of any kind or nature whatsoever.

3. If any Documents required herein are withheld under claim of privilege or are not produced for whatever reason, you are required at the time of responding to this subpoena to separately state in writing and with specificity for each Document withheld from production (i) the claim of privilege or other reason asserted for withholding each such Document, and (ii) all information supporting the claim of privilege or other reason for withholding asserted as to each such Document, including without limitation the type or nature of the Document withheld (e.g., letter, memorandum, email, etc.), its author and all recipients (including any and all addressees and Persons to whom the Document was copied or blind copied, as well as Persons to whom the Document was distributed or given or shown though not reflected on the Document as a recipient), the date of the Document, and a description of the substance of the Document, all in a manner sufficient to allow each Document to be described to the Court in order for the Court to rule on the

claim of privilege or other reason asserted for withholding it from production. You are further required to provide all responsive information that is not subject to a claim of privilege, or other reason for nonproduction, by excising or otherwise protecting the portions for which a privilege is asserted, if such a technique does not result in disclosing the contents of the portions for which some privilege is asserted.

DOCUMENTS AND THINGS TO BE PRODUCED

CATEGORY NO. 1: All Documents and Communications related to Smartmatic.

CATEGORY NO. 2: All Documents and Communications related to any software hardware, firmware, or other product distributed by Smartmatic.

CATEGORY NO. 3: All Documents and Communications between You and Smartmatic.

CATEGORY NO. 4: All Documents and Communications concerning the Joint Statement, including all documents supporting the assertion in the Joint Statement that "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised."

CATEGORY NO. 5: All Documents and Communications related to any actual, suspected, or reported instance of Unauthorized Access to Electronic Election Equipment located in the United States, between October 1, 2020 and November 30, 2020.

CATEGORY NO. 6: All Communications to You from Halderman or from any person acting on behalf of Halderman.

CATEGORY NO. 7: All Communications from You to Halderman or to any person acting on behalf of Halderman.

CATEGORY NO. 8: All Documents and Communications related to Halderman.

CATEGORY NO. 9: All Documents and Communications between You and the Office of the Georgia Secretary of State related to the Halderman Report.

CATEGORY NO. 10: All Documents and Communications between You and the office of any state's Secretary of State, other than Georgia, related to the Halderman Report.

CATEGORY NO. 11: All Documents and Communications between You and any federal agency related to the Halderman Report.

CATEGORY NO. 12: All Documents and Communications related to any testing or examination of any Electronic Election Equipment related to any vulnerability identified in the Halderman Report.

CATEGORY NO. 13: All Documents and Communications related to any Cybersecurity vulnerabilities or weaknesses of Ballot Marking Devices.

CATEGORY NO. 14: All Documents and Communications related to any Cybersecurity vulnerabilities or weaknesses in the Auto-Cast system configuration for Ballot Marking Devices.

EXHIBIT B

JOINT STATEMENT FROM ELECTIONS INFRASTRUCTURE GOVERNMENT COORDINATING COUNCIL & THE ELECTION INFRASTRUCTURE SECTOR COORDINATING EXECUTIVE COMMITTEES

Original release date: November 12, 2020

WASHINGTON – The members of Election Infrastructure Government Coordinating Council (GCC) Executive Committee – Cybersecurity and Infrastructure Security Agency (CISA) Assistant Director Bob Kolasky, U.S. Election Assistance Commission Chair Benjamin Hovland, National Association of Secretaries of State (NASS) President Maggie Toulouse Oliver, National Association of State Election Directors (NASED) President Lori Augino, and Escambia County (Florida) Supervisor of Elections David Stafford – and the members of the Election Infrastructure Sector Coordinating Council (SCC) – Chair Brian Hancock (Unisyn Voting Solutions), Vice Chair Sam Derheimer (Hart InterCivic), Chris Wlaschin (Election Systems & Software), Ericka Haas (Electronic Registration Information Center), and Maria Bianchi (Democracy Works) - released the following statement:

“The November 3rd election was the most secure in American history. Right now, across the country, election officials are reviewing and double checking the entire election process prior to finalizing the result.

“When states have close elections, many will recount ballots. All of the states with close results in the 2020 presidential race have paper records of each vote, allowing the ability to go back and count each ballot if necessary. This is an added benefit for security and resilience. This process allows for the identification and correction of any mistakes or errors. **There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised.**

“Other security measures like pre-election testing, state certification of voting equipment, and the U.S. Election Assistance Commission’s (EAC) certification of voting equipment help to build additional confidence in the voting systems used in 2020.

"While we know there are many unfounded claims and opportunities for misinformati process of our elections, we can assure you we have the utmost confidence in the security and integrity of our elections, and you should too. When you have questions, turn to elections officials as trusted voices as they administer elections."

###

Topics: Election Security

Keywords: CISA, Election security

Last Published Date: November 12, 2020

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

EXHIBIT D

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

DONNA CURLING, ET AL., *Plaintiffs*, v. BRAD RAFFENSPERGER, ET AL., *Defendants*.	No. 1:17-CV-2989-AT NOTICE

The undersigned counsel respectfully submit this notice on behalf of the United States Cybersecurity and Infrastructure Security Agency (CISA) in response to matters raised at the Court's February 2, 2022 hearing regarding CISA's Coordinated Vulnerability Disclosure (CVD) process. Specifically, CISA writes to provide additional information on the CVD process and its timeline, to reiterate its commitment to ensuring election security and completing the CVD process as quickly as feasible, and to notify the Court of CISA's view that premature disclosure of Dr. Halderman's report, even in redacted form, could, in the event any vulnerabilities ultimately are identified, assist malicious actors and thereby undermine election security. As explained herein, CISA thus respectfully submits that public disclosure, even in redacted form, should await completion of the normal CVD process and proposes that it notify the Court within 30 days of any status updates regarding the process and its anticipated timeline, as well as any updates regarding CISA's views as to scope and information to be included in a future public disclosure.

CISA understands that, during the February 2nd hearing, the Court authorized disclosure to CISA of an unredacted report prepared by Dr. Halderman for the purpose of CISA

undertaking its CVD process. CISA received an unredacted copy of the report from Dr. Halderman on February 2nd, and counsel for Plaintiffs shared the unredacted report with Dominion Voting Systems on February 4th. The report discusses potential vulnerabilities in Dominion ImageCast X ballot marking devices. *See generally* ECF 1177-1 ¶ 2.

Now that the report has been shared among Dr. Halderman, CISA, and Dominion, CISA has commenced its CVD process, which is described in detail in CISA's January 20, 2022 letter, *see* ECF No. 1269. CISA understands and shares the parties' urgency with completing this work, and will prioritize its completion as expeditiously as possible. As confirmed in CISA's letter, the CVD process requires the agency to coordinate between and work with the reporting source of the potential vulnerabilities (here, Dr. Halderman) and the vendor (here, Dominion), to analyze the potential vulnerabilities, including the risk they present; develop mitigation measures to mitigate the risk of the potential vulnerabilities, as needed; facilitate sufficient time for affected end users to obtain, test, and apply any recommended mitigation measures prior to full public disclosure of the potential vulnerability; and strive to ensure accurate and objective disclosures by the vendors. *See generally id.*[1] A range of factors—such as the potential impact on critical infrastructure (*e.g.*, election equipment), the availability of effective mitigations, the feasibility of developing an update or patch, the estimated time necessary for affected end users to obtain, test, and apply the patch, or other situations that require changes to established standards—may result

[1] CISA is also aware that, prior to and separate from the commencement of the CVD process, the Court imposed a protective order on dissemination of Dr. Halderman's report, as applied to parties in the litigation. As noted in CISA's letter, ECF No. 1269 at 2-4, the CVD process requires sharing and dissemination of vulnerability information. CISA understands the Court to have authorized disclosure of Dr. Halderman's report to CISA for the purpose of following its normal process, including, as appropriate, any information-sharing with Dr. Halderman, Dominion, affected end users, and, at the conclusion of the process, with the public. *See* Feb. 2, 2022 Hr'g Trans. at 5:12-20; 9:19-10:2.

in shifts to both the timeline and process. *See id*. Depending on what is discovered, CISA may need to coordinate with one or more affected end users, including states and municipalities using the same technology, early in the CVD process.

Both from the transcript of the February 2nd hearing and from a February 3rd conversation between undersigned counsel and the parties, CISA understands that the parties to this case requested a redacted version of Dr. Halderman's report to be released publicly as soon as possible. Specifically, the plaintiffs apparently request release of the redacted report within 30 days, while the State would prefer immediate (or as soon as practicable) release. CISA also understands that the Court would like to ascertain how quickly CISA can complete its process and whether CISA will be prepared to provide its views on what information may be released publicly without compromising security and what information should be withheld.

As to the timeline for the CVD process, CISA is not able to provide a definitive answer at this point. As with all of its CVD work, CISA's goal is to facilitate an assessment of the potential vulnerabilities in a coordinated way that minimizes risk. If warranted, CISA will coordinate with the vendor during development of any patches or other mitigation measures necessary to address any identified vulnerabilities. The rapidity with which that can be completed depends largely on the scope of any identified vulnerabilities, the actions and responses among participants in the process (*i.e.*, Dr. Halderman, Dominion, and states and municipalities using the same technology), the mitigation measures any identified vulnerabilities may warrant, and other factors, including the feasibility of, and timeline for, developing any needed update(s) or patch(es). Any mitigation measures also must be made available to affected end users—*i.e.*, both Georgia and other states/municipalities using the same technology—and must be obtained, applied, and tested by those stakeholders, as well as, in some cases, certified for use by those

stakeholders. Election security is a top priority; CISA is thus committed to taking these steps expeditiously and will seek to complete the process as promptly as possible. But the timeline also depends on the actions of a range of other actors outside CISA's control. A 30-day timeline may be impractical in this situation, despite best efforts and prioritization of this work.

CISA understands the urgency given the upcoming elections in which this voting equipment is presently planned to be used. Yet CISA can neither control how quickly any necessary mitigation measures are developed, made available, and implemented, nor at this time can CISA anticipate with any degree of reasonable certainty how long the process may take. This was communicated by undersigned counsel to counsel for the parties and counsel for Dominion during the February 3, 2022 conference call.

As to what can be released publicly, CISA supports public disclosure of any vulnerabilities and their associated mitigations, subsequent to any applicable mitigation measures being developed and applied, consistent with the CVD process. ECF No. 1269 at 3. As explained in CISA's January 20, 2022 letter, CISA carefully stewards sensitive data made available to the agency as part of the CVD process, maintaining confidentiality until disclosure to affected end users and the public at large is warranted. This enables key vulnerabilities to be addressed, while also preserving the confidentiality of sensitive proprietary information. Consistent with this approach, CISA typically would not release a report such as Dr. Halderman's at the conclusion of the CVD process; it would, however, disclose necessary information about any vulnerabilities and associated mitigations.

CISA is particularly concerned about dissemination of potential vulnerabilities—even in redacted form—before CISA and the vendor have been able to address them through appropriate mitigation action. Such premature disclosure increases the risk that malicious actors may be able

to exploit any vulnerabilities and threaten election security. CISA respectfully submits that, in order to best promote the security of the nation's critical infrastructure, any vulnerabilities should be disclosed—with the maximum appropriate transparency—in accordance with the CVD process. CISA's goal is to disclose any confirmed vulnerabilities and associated mitigations to the public in a coordinated way, so the entire cyber ecosystem can benefit while minimizing the risk of harm to election security.

For these reasons, CISA respectfully submits that public disclosure, even in redacted form, should await completion of the normal CVD process. CISA is committed to prioritizing this work and ensuring it is given the attention it deserves. CISA proposes that it notify the Court within 30 days of any status updates regarding the process or the anticipated timeline for completion, as well as any updates regarding CISA's views as to scope and information to be included in a future public disclosure.

Respectfully submitted,

BRIAN M. BOYNTON
Acting Assistant Attorney General

BRIGHAM J. BOWEN
Assistant Branch Director

/s/ Kate Talmor
KATE TALMOR
Trial Attorney
Civil Division
Federal Programs Branch
US Department of Justice
1100 L St., NW
Washington, DC 2005
202-305-5267
kate.talmor@usdoj.gov

EXHIBIT 5

IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Election Infrastructure Insider Threat Mitigation Guide

INTRODUCTION

Individuals entrusted with access to election infrastructure can, at times, represent potential risks to the confidentiality, integrity, and availability of election systems and information. This includes current and former employees, volunteers, contractors, and any other individual who has been granted privileged access to election systems and information. Across all critical infrastructure sectors and in virtually every organizational setting, trusted insiders have the potential to cause intentional or unintentional harm.

Practices that deter, detect, or prevent harm caused by insiders are an integral part of conducting secure elections. This guidance assists those working in the election infrastructure subsector to improve existing insider threat mitigation practices and establish an insider threat mitigation program, and summarizes and expands upon select guidance from previously issued CISA resources on insider threat mitigation for critical infrastructure stakeholders.

DEFINING INSIDER THREATS[1]

Insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

Unintentional Threats

Insider threats can be unintentional, including cases of negligence or accidents.

- **Negligent**: Insiders can expose an organization to harm by their carelessness. Insiders of this type are generally familiar with security and/or IT policies but choose to ignore them, creating a risk to the organization. Negligent insiders are usually complacent or show an intentional disregard for the rules. They exhibit behaviors which can be witnessed and corrected.
- **Accidentals**: Even the best employee can make a mistake causing an unintended risk to the organization. Organizations can implement strategies to limit risk, but accidents may still occur. While accidents can't be fully prevented, risk can be reduced through training and appropriate controls.

Intentional Threats

Insiders can intentionally take actions that harm an organization for personal benefit or to act on a personal grievance. Some intentional insiders are motivated by a disgruntlement related to a perceived grievance, ambition, or financial pressures. Others may have a desire for recognition and seek attention by creating danger or divulging sensitive information. They may even think they are acting in the public good.

Other Threats

In addition to insider threats involving only insiders at an organization, insider threats may also involve individuals external to the organization. These collusive and third-party threats may be either unintentional or intentional.

- **Collusion**: This threat occurs when one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, sabotage, or a combination of these. This type of insider threat can be challenging to detect, as the external actors are typically well-versed in security practices and strategies for avoiding detection.
- **Third-Party Threats**: Third-party threats are associated with contractors or vendors who are not formal members of an organization, but who have been granted access to facilities, systems, networks, or people to complete

[1] Definitions sourced from: "Insider Threat Mitigation Guide." Cybersecurity and Infrastructure Security Agency, 2020. https://www.cisa.gov/sites/default/files/publications/Insider Threat Mitigation Guide_Final_508.pdf

their work. This type of threat can involve collusion among multiple third-party entities. Third-party threats may be direct, where specific individuals compromise a targeted organization, or indirect, where there may be flaws or outdated systems exposing the organization to unintentional or malicious threat actors.

Examples of Unintentional Threats

- Allowing someone to "piggyback" through a secure entry point
- Misplacing or losing portable storage devices or media containing sensitive information
- Ignoring messages to install new software updates or security patches
- Mistyping an email address and accidentally sending a sensitive business document externally
- Unknowingly or inadvertently clicking on a hyperlink or phishing email
- Improperly disposing of sensitive documents or data

Examples of Intentional Threats

- Attempting to alter or destroy ballots, mail-in ballot envelopes, registration forms, or other core election documents
- Attempting to violate ballot secrecy
- Attempting to alter or destroy elections data, including voter registration data
- Allowing an unauthorized person to access election equipment, systems, assets, or data
- Turning off security cameras or access control systems
- Stealing election equipment or data
- Leaking confidential information to the press or public
- Intimidating or threatening other staff

Expressions of Insider Threat

Insider threats manifest in various ways, including violence, espionage, sabotage, theft, and cybersecurity incidents.

- **Cybersecurity Incidents**: These include a range of actions, which may include theft, espionage, violence, or sabotage, dealing with anything related to technology, virtual reality, computers, devices, or the internet. These actions are undertaken using a variety of vectors such as viruses, data breaches, denial of service attacks, malware, or unpatched software, and can be either unintentional or intentional.
- **Violence**: An act of violence, threats of violence, or other threatening behavior that creates an intimidating, hostile, or abusive environment. Insider violence includes criminal or destructive threats, which precede a physical attack, and damage infrastructure or harm the health and safety of an individual or organization. This can include terrorism or workplace/organizational violence.
- **Espionage**: The practice of spying on a foreign government, organization, entity, or person to covertly or illicitly obtain confidential or sensitive information for military, political, strategic, or financial gain. This includes criminal, economic, or government espionage.
- **Sabotage**: Involves deliberate actions aimed at harming an organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or modifying or deleting code to disrupt operations.
- **Theft**: Theft involves multiple types of stealing, most often involving finance or intellectual property. Financial crime is the unauthorized taking or illicit use of a person's, business', or organization's money or property with the intent to benefit from it. Theft also includes intellectual property theft, or the robbery of an individual's or organization's ideas, inventions, and/or creative expressions. Digital systems containing large quantities of customer data or intellectual property may be more appealing to bad actors.

WHAT IS MDM?

CISA uses the following definitions for mis-, dis-, and malinformation (MDM). MDM can originate from both foreign and domestic sources.

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Insider Threats and Mis-, Dis-, and Malinformation

The information environment surrounding elections, and particularly the spread of election-related mis-, dis-, and malinformation (MDM), may provide additional motivation for insider threats. MDM content is often designed to elicit a strong emotional response from the consumer and bypass logical reasoning to incite action, whether the action is simply spreading the content further on social media or taking action in the real world, including acts or threats of violence. A common tactic deployed by both foreign and domestic MDM actors is to reinforce a strong sense of belonging, community, and in-group mentality among those who regularly consume their content. In instances where an individual already has a grievance with an organization or is experiencing other stressors in their life, MDM narratives may provide an alternate interpretation of reality that appears preferable to real life. This vulnerability can lead to or exacerbate insider threats.

While election infrastructure stakeholders cannot predict or fully control the information environment around elections, they can educate their staff, volunteers, and vendors about MDM narratives and tactics. Ongoing training and education opportunities are especially important for non-full-time staff, who may not join the organization with full knowledge of election processes or how they may be impacted by MDM content. Similarly, election infrastructure stakeholders can mitigate the impact of MDM narratives through proactive and consistent communication with the public about election processes. Such communication can help avoid fueling MDM narratives and build organizational resilience against them. When communicating about election processes, election infrastructure stakeholders should aim to provide straightforward, concise information without being overly detailed or causing more confusion.

The current MDM environment, at the local, national, and international level, should be considered when assessing insider threats. Transparent communication, in conjunction with the prevention and detection measures described below, can help staff understand and perform their role, connect it to the organization's mission to administer secure elections, and stay resilient against potential MDM narratives that undermine that mission and potentially incite insiders to cause intentional harm.

BUILDING AN INSIDER THREAT MITIGATION PROGRAM

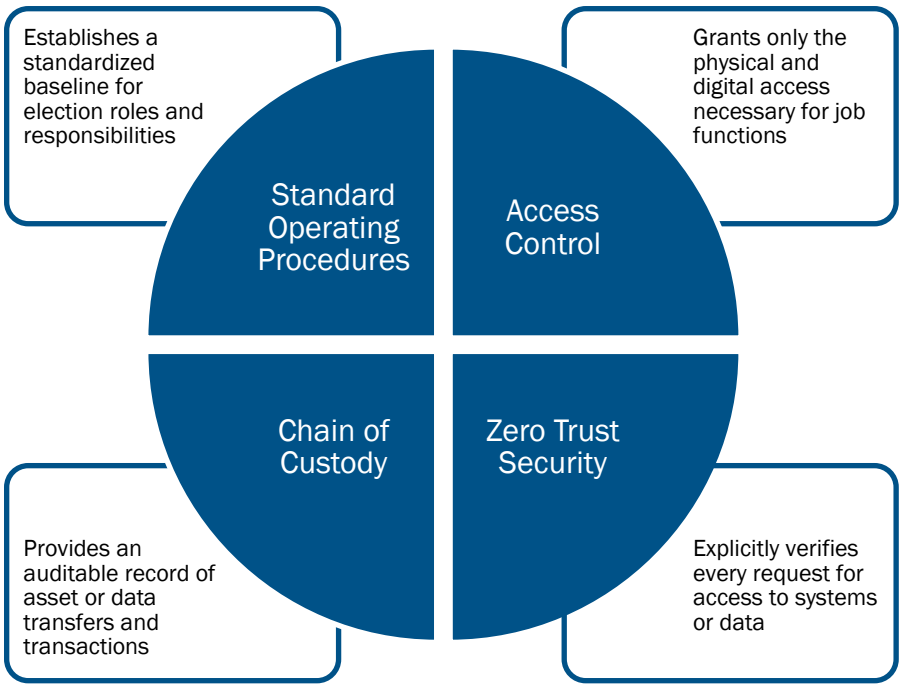
Election officials and their private sector partners regularly employ practices designed to deter, detect, or prevent harmful acts by insiders -- whether or not they use the term "insider threat" or have articulated their approach and practices in a documented program. From handling ballots in teams of two, to robust chain-of-custody procedures, to the presence of observers during voting and counting, many longstanding core election practices have been designed with insider threat mitigation in mind. Nevertheless, election infrastructure stakeholders may benefit from documenting their approach and establishing a more formalized insider threat mitigation program. Such actions can help identify gaps in current practices and inform the organization's broader approach to risk management.

Successful insider threat mitigation programs employ proven practices, strategies, and systems that limit and track access across organizational functions, services, and applications. Those practices and systems limit the amount of damage an insider can do, whether the act is intentional or unintentional. A holistic, multi-layered approach to insider threat mitigation combines physical and digital security with personnel engagement. An effective mitigation program aims to understand the insider's interaction within an organization, track the interaction as appropriate and permitted by law, and intervene if the interaction poses a threat to the organization. An organization's insider threat mitigation program is an essential component of the broader organizational risk management plan.

A strong foundation for insider threat prevention and mitigation comes from a set of values that are shared and acted upon by everyone in the organization. **Organizations should promote a positive climate of accountability, transparency, and trust.** Organizational culture should also reinforce employee reporting as a core component of securing the environment.

Key Elements of Election Infrastructure Insider Threat Mitigation Programs

From a foundation of a proactive and supportive culture, election infrastructure stakeholders can implement several proactive and preventive measures to reduce the risk and impact of insider threat activity. While each aspect is individually important, they are most effective when implemented together to create a comprehensive, resilient election administration environment. Key elements of election infrastructure insider threat mitigation programs include: establishing robust standard operating procedures (SOPs), managing physical and digital access control, deploying zero trust security principles, and implementing chain of custody processes.



Standard Operating Procedures

Establishing and implementing SOPs primarily helps prevent unintentional insider threats due to negligence or accidents. SOPs outline how organizational functions should be performed and standardize the various tasks and responsibilities associated with different roles, increasing the quality and consistency of work across staff. Especially in an election environment, where volunteers and third-party vendors turnover regularly, SOPs can help employees onboard quickly, understand the expectations of their role, and successfully perform their duties. Further, SOPs create a baseline against which to measure outcomes and identify areas for increased efficiency and improvement.

SOPs for each role or responsibility should clearly document the steps needed to perform the activity successfully. This includes providing sequential steps for task completion, showing visuals and examples, and specifying the checklists and logs necessary for verification. Incomplete or nonexistent SOPs may cause staff to develop their own procedures, which may induce additional risk. SOPs therefore limit *ad hoc* decision making and can help speed the remediation process should issues arise.

Access Control

Physical and digital access control systems both prevent and detect insider threats. Physical access controls may include limiting access to facilities, equipment, devices, tamper-evident seals and bags, and other assets as well as providing video surveillance of physical assets. Digital access controls grant access only to necessary systems, assets, data, or applications related to an individual's job or function. In both cases, access logs, control forms, and surveillance video provide auditable records of who accessed a physical or digital asset, as well as when it was accessed. Overall, access control systems prevent any one individual from gaining entry to all assets within an organization, reducing potential harm to physical or digital systems. If an incident is suspected, access logs and controls forms can help identify who is responsible for potentially harmful behavior.

Access control systems should apply the **principle of least privileged access** to grant all individuals (full-time staff, volunteers, and vendors) access only to systems and data required to perform their essential functions. Access privileges may change leading up to an election or other key dates. Additionally, organizations should ensure that access is promptly revoked when an individual concludes their work or leaves the organization (e.g., turning off facility access for vendors once they complete routine maintenance).

A key challenge around access control for election officials is access to the state voter registration database system. The state may not know who has access within each local election office, so it is important for jurisdictions and state offices to work together to regularly confirm and update a list of authorized users and associated privileges.

Zero Trust Security Principles

A zero trust approach to security is based on the principle of "always verify." Instead of assuming that everything that happens on an organization's networks and systems is safe, the zero trust approach assumes that a breach has or will occur and verifies each request as though it is unauthorized. Previously, in many organizations, the security of digital assets was closely tied to the physical location where they were stored and universal trust in all members of the organization. In other words, all devices in an office and all staff users could access most information, systems, and data. This implicit trust of devices or users made it easy for insider threats to manifest in an organization undetected. In contrast, the zero trust approach explicitly verifies every request for access, regardless of where it originates or what resource it accesses. Many digital systems now include zero trust security features that can be turned on, such as always requiring users to enter their password rather than storing it in the device's memory. Election infrastructure stakeholders may also consider procedures like implementing the "two-person rule" (require at least one observer to be present) or working in bipartisan teams when accessing sensitive resources.

Visit https://zerotrust.cyber.gov/ for additional guidance on zero trust implementation from CISA and the Office of Management and Budget (OMB).

Chain of Custody

Chain of custody is a transparent process to track the movement and control of physical and digital assets by documenting each person and organization that handled an asset, sensitive equipment, or data; the date and time it was collected, transported, or transferred; and why the asset was handled. While not unique to elections, chain of custody plays a vital role in ensuring the integrity of an election and providing evidence in the event an insider threat is detected, as well as improving remediation time if an incident occurs. Without robust chain of custody practices, election systems equipment, assets, or data at rest or in transit could be unknowingly accessed and manipulated by threat actors.

Elections are complex, and there are many functions that make up the intricate process of conducting an election. At every point where data, media, or equipment are entered, accessed, transferred, transmitted, or stored, there is an opportunity for error or risk. Robust chain of custody practices reduce this risk by creating an auditable trail of assets throughout the election process.

To address risk and improve security and resilience, election infrastructure stakeholders can utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to establish chain of custody standards, guidelines, and practices. NIST outlines a five-step process to identify assets and risks, protect systems, detect incidents, respond to breaches, and recover.

Example: a chain of custody procedure could require that at least two people sign all equipment, transported materials, or media access logs: the primary user and a witness who ensures the equipment, , media, or other assets were appropriately handled. Absent this requirement, it may be difficult to verify who accessed or transported the equipment, media, or other assets and for what purpose.

Establishing and maintaining necessary standard operating procedures, access controls, zero trust security, and chain of custody procedures are necessary facets of election administration. Further, they must be reviewed, tested, and audited before, during, and after elections. Altogether, these measures support the integrity, reliability, and security of an election, providing the evidence to build public confidence in the process.

ELECTION INSIDER THREATS IN FOCUS

In most jurisdictions, election officials administer elections with assistance from temporary or seasonal staff, volunteers, vendors, and contractors. Similar to potential threats posed by full-time staff, such individuals may pose an insider threat. Therefore, election officials should ensure that all individuals involved in elections are considered, based on their specific roles and responsibilities, when developing an insider threat mitigation program.

Vendors and Contractors

Vendors and contractors should be held to the same level of security standards as employees. Election officials should ensure that they build into their procurement processes and contracting requirements the same safeguards that they hold their own employees to. When acquiring new contracted services, security requirements and minimum qualifications should be built into requests for proposals and in the final contractual agreements, such as mandatory background checks for all individuals who will be working on the contract.

Vendors and contractors will likely have the same or greater physical and/or digital access to certain critical data that full-time staff do, and they therefore bring similar, if not increased, risk to election infrastructure. Election officials should consider restricting or eliminating remote access to election systems or assets by contractors, limiting access to only systems and data required to perform the contracted service, and when possible, having a government official present when contractors access critical systems or data (but at minimum always require that at least two people are present). When possible, segregate vendor and contractor accounts from those of regular employees and utilize devices managed by the organization to prohibit untrusted devices on the network. Consider providing individuals with a colored lanyard, badge, vest, or similar item when they are working at government facilities so it is easy for all to identify who should or should not be in secure areas.

Temporary Staff, Seasonal Staff, and Volunteers

Most election offices rely on temporary, seasonal, and/or volunteer workers to conduct polling operations, including the operation of election equipment and transporting sensitive media or election materials, process voter registration forms, handle mail-in ballot request forms, manage mail-in ballots, and other election administration tasks. Building a successful team of temporary and volunteer staff starts with the recruitment of individuals who understand the mission of the organization and possess a high degree of accountability for their role. Upon joining the organization, all new members should be required to sign a code of conduct that clearly articulates expected behavior and outlines consequences for violations.

In addition to the considerations above, temporary staff and volunteers should be retrained on systems, data, and security practices prior to every election. It is especially important to provide updated training on MDM trends, including MDM risks specific to the state or jurisdiction. Finally, SOPs and chain of custody procedures should include guidance for all role types, including temporary staff and volunteers. This may include use of the two-person rule, or control forms, which can be an effective measure for temporary staff and volunteers to check each other's work, deter harmful behavior, and verify compliance.

DETECTING AND IDENTIFYING INSIDER THREATS

Even the most robust preventive and protective measures cannot fully eliminate the risk of intentional or unintentional insider threats. Therefore, it is important for election infrastructure stakeholders to routinely test and audit their procedures, which will aid in identifying procedural gaps and responding to evolving threats in elections. Threat detection takes place through both human review and technical tools that monitor for the presence of threat indicators.

As those who perpetrate violence or steal data often share their plans or grievances with others before acting, coworkers, peers, friends, neighbors, family members, or casual observers are frequently positioned to have insight into and awareness of predispositions, stressors, and behaviors of insiders who are considering malicious acts.

Each individual has a baseline of behaviors and straying from their norm could be an indication that something about them has fundamentally changed. Important to the process of identifying potential threat indicators is understanding that **behavior is what matters most**, not the motivation. The presence of political, religious, ideological, financial, or revenge-based motivations helps to understand what drives an individual to act, but the individual's behavioral indicators are the key to determining whether they warrant additional consideration, monitoring, or assessment as a potential threat.

Insider Threat Preventative Measures as Detection Mechanisms

Preventive measures against insider threats, including SOPs, access control systems, zero trust security, and chain of custody, also contribute to detecting and identifying threats by establishing transparent, auditable election systems and processes. However, effective detection via these measures requires human understanding and oversight to ensure they are being applied appropriately and audited routinely to identify outliers for further investigation. Having preventive measures in place means little if they are not consistently used.

Each measure can aid threat detection in the following ways:

- **Standard Operating Procedures**: SOPs and best practices provide a common baseline for a team to measure against and detect when best practices are not being followed.
- **Access Control Systems**: These systems generate access logs and security footage that can be reviewed to verify access to both physical and digital systems and detect if unauthorized access has occurred.
- **Zero Trust Security**: Like access control systems, zero trust security measures will provide a record of access to digital systems and data. By validating a user's identity at every request for access, zero trust measures provide granular information about access.
- **Chain of Custody**: Chain of custody produces an auditable record of an asset's transfers and transactions, enabling detection of a potential threat if there is a gap in the chain.

Continuous Monitoring

Monitoring for insider threats, as well as for any issues with the systems in place, should be continuous. This involves a combination of human and digital tools, underpinned by a strong organizational culture of proactive reporting. All employees have a part to play in the process to hold themselves and others accountable for following established procedures. Through ongoing, proactive monitoring, even the most organized and well-resourced election office may find practices that are outdated or not consistently followed, leaving the organization exposed to risk if not properly addressed. Finally, all procedures and practices, including any monitoring programs, should be regularly reviewed and updated for compliance with applicable federal, state, and local laws.

Auditing

Internal audits of all election and business processes should be a routine part of election administration before, during, and after an election. Audits validate whether measures such as access control and chain of custody are functioning properly, collecting and maintaining necessary data or equipment, and being used appropriately by staff. They also provide the opportunity to review records (access logs, security footage, chain of custody forms, etc.) and identify any potential gaps or areas for improvement. Audits should be used to look for evidence that demonstrates the effectiveness and durability of procedures, processes, systems, and training practices.

Election infrastructure stakeholders are encouraged to identify a timeline for periodic audits that makes sense for their workflow and capacity; smaller and more frequent internal audits of different processes may be less disruptive than one major year-end audit. It is recommended to build audits into an organization's SOPs. Election infrastructure stakeholders should not wait for external requests to perform audits of their systems and processes.

Transparency

The election process is transparent and open to public observation, which provides a unique strength compared to many other critical infrastructure areas. Allowing the public to assist with and observe the election process can help illuminate points where the process is unclear and provide opportunities to make improvements. From the perspective of insider threats, public participation may result in detecting "false positives" due to lack of clarity or understanding. This underscores the importance of documenting procedures thoroughly, testing and auditing them, and educating the public on them.

ASSESSING INSIDER THREATS

Insider threat assessment is the process of compiling and analyzing information about a person of concern who may have the interest, motive, intention, and capability of causing harm to an organization or persons, with the goal of preventing an insider incident in any of its expressions. The insider threat management team conducting the investigation should answer several key questions:

1. *Is there evidence to suggest the person of concern poses a threat?*
2. *What type of threat does the person of concern pose?*
3. *Is the person of concern moving towards committing a malicious act?*

Non-Emergency Intervention

If the initial screening of these three questions indicates that there is not an immediate potential for a threat, then the organization should begin, to the extent authorized by law, a deeper investigation to gather information, evaluate the risk, and determine next steps. During the investigation stage, the insider threat management team may need to consider consulting with an external threat assessment professional, consulting with legal counsel, and/or initiating coordination with law enforcement, as necessary.

The purpose of the investigation is to gather evidence (including from access control systems, security logs, and chain of custody forms), determine the person of concern's baseline behavior and changes from it, analyze the risk of moving towards a malicious act, and document the findings. Based on the investigation, the team can determine next steps, which may include, but are not limited to, watching and waiting, changing or restricting access privileges, taking administrative action such as suspension or termination, assisting with finding outside counseling or support, and/or reporting to law enforcement.

Emergency Intervention

If it is determined that emergency intervention is required based on the initial screening, then the organization should take immediate action, including calling for assistance from first responders or law enforcement if necessary.

In the event of physical violence or sabotage, the team should initiate the organization's Incident Response Plan, skip the initial screening, contact appropriate authorities, and begin an investigation as soon as it is safe to do so. For cases of targeted violence or sabotage, emergency intervention can sometimes result in the need to evacuate a location or facility, initiate a lockdown, or shelter in place. The organization should have plans in place for each response and coordinate across the organization for immediate action.

MANAGING INSIDER THREATS

As discussed above, effective insider threat mitigation requires that organizations foster a positive, supportive culture that encourages employees to report unusual behavior. Integral to this goal is a transparent and consistent process for reporting, where both staff and the public know that their reports will be acknowledged, taken seriously, and handled appropriately. Election infrastructure stakeholders should emphasize that contribution toward this goal is shared by everyone in the community, including staff, vendors, and volunteers involved in administering elections. Programs that encourage early reporting and intervention increase the likelihood that a threat can be mitigated or deescalated.

Once an issue has been resolved or mitigated, consider organizing a debrief session for appropriate stakeholders to discuss the issue, the steps that were taken to mitigate it, and areas for improvement. This helps reinforce a culture of engagement and awareness and enables the entire team to be better prepared in the future.

FURTHER RESOURCES

Insider Threat Mitigation

- CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute: Offers written products for insider threat mitigation across a variety of organizational settings.
- I Insider Threat Mitigation Resources | CISA: Shares overarching guidance to aid individuals, organizations, and communities in understanding insider threats and improving or establishing an insider threat mitigation program.
- Insider Threat Mitigation Guide | CISA: Provides comprehensive guidance for organizations of all sizes in support of the establishment or enhancement of an insider threat mitigation program. The information within the guide is scalable and allows for the consideration of the level of maturity and size of the organization.
- Insider Risk Self-Assessment | CISA: A tool to assist owners and operators or organizations, especially small and mid-sized ones who may not have in-house security departments, to gauge their vulnerability to an insider threat incident. The tool is a downloadable PDF that asks users key questions about their existing enterprise, focusing on the domains of Program Management, Personnel and Training, and Data Collection and Analysis.
- National Insider Threat Task Force (NITTF): Helps federal departments and agencies identify best practices for detecting, deterring, and mitigating emerging threats. NITTF also provides a variety of products and resources applicable to state, local, tribal, and territorial and critical infrastructure entities.
- FBI Insider Threat: An Introduction to Detecting and Deterring an Insider Spy: An introduction for managers and security personnel on behavioral indicators, warning signs, and ways to detect and deter insiders from compromising organizational trade secrets and sensitive data more effectively.

Mis-, Dis-, and Malinformation (MDM)

- MDM Resource Library: CISA's Mis-, Dis-, and Malinformation (MDM) team is charged with building national resilience to MDM and foreign influence activities. Through these efforts, CISA helps the American people understand the scope and scale of MDM activities targeting elections and critical infrastructure and enables them to take actions to mitigate associated risks.

Cybersecurity for Critical Infrastructure

- Framework for Improving Critical Infrastructure Cybersecurity | NIST: Provides a framework and path forward for critical infrastructure stakeholders to assess cybersecurity risks, improve risk management, and prioritize and achieve cybersecurity objectives.
- Supply Chain Risk Management Practices for Federal Information Systems and Organizations | NIST: Expands on cybersecurity risk management guidance by diving deeper into information and communications technology (ICT) supply chain risks and how to identify, assess, and mitigate them.

Chain of Custody

- Chain of Custody and Critical Infrastructure Systems | CISA: Overview of what chain of custody is, potential impacts and risks of broken chain of custody, and an initial framework for securing physical and digital assets for those working on critical infrastructure systems.
- Chain of Custody Best Practices | EAC: Best practices in chain of custody practices specifically for election officials.
- Chain of Custody – General Terminology and Models: International Organization for Standardization (ISO 22095:2020) guidance on chain of custody processes.

Conducting Internal Audits

- Unique Aspects of Internal Auditing in the Public Sector | IIA: This guidance will enable internal auditors to plan and perform internal audit engagements with an understanding of the unique roles and principles of public sector organizations.
- Assessing Organizational Governance in the Public Sector | IIA: Overview of how internal auditors can assess and make appropriate recommendations for improving governance activities and processes for public sector organizations.
- Creating an Internal Audit Competency Process for the Public Sector | IIA: This guide helps ensure that an organization's audit function has the collective knowledge, skills, and other competencies necessary to complete planned audits.

Election Technology Procurement

- A Guide for Ensuring Security in Election Technology Procurements | CIS: A guide on procuring computer hardware, software, and services for election administration.
- Managing Cybersecurity Supply Chain Risks in Election Technology | CIS: This guide for election technology providers provides best practices for specific problem areas identified by the election community.

EXHIBIT 6

Cybersecurity and Infrastructure Security Agency

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

July 28, 2020; 1400 EDT.

ELECTION INFRASTRUCTURE CYBER RISK ASSESSMENT

Fair and free elections are a hallmark of American democracy. The American people's confidence in the value of their vote is reliant on their confidence in the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA's) highest priorities. CISA is working collaboratively in coordination with our federal partners, with those on the front lines of elections—state and local governments, election officials, and vendors—to manage risks to the Nation's election infrastructure. In this paper, CISA assesses risk to election infrastructure in order to assist the election community in understanding and managing risk to their critical systems.

To complete this work, CISA's National Risk Management Center (NRMC) assessed multiple criteria that quantify the scale of election infrastructure cyber risk, including machine preparation, device networking, and the centralization of infrastructure components. CISA NRMC also assessed additional risk criteria related to voter registration, voting machines, and electronic submission of ballots.

KEY FINDINGS

Compromises to the integrity of state-level voter registration systems, the preparation of election data (e.g., ballot programming), vote aggregation systems, and election websites present particular risk to the ability of jurisdictions to conduct elections.

When proper mitigations and incident response plans are not in place, cyber attacks on the availability of state or local-level systems that support same day registration, vote center check-in, or provisional voting also have the potential to pose meaningful risk on the ability of jurisdictions to conduct elections.

While compromises to voting machine systems present a high consequence target for threat actors, the low likelihood of successful attacks at scale on voting machine systems during use means that there is lower risk of such incidents when compared to other infrastructure components of the election process.

U.S. election systems are comprised of diverse infrastructure and security controls, and many systems invest significantly in security. However, even jurisdictions that implement cybersecurity best practices are potentially vulnerable to cyber attack by sophisticated cyber actors, such as nation-state actors.

Disinformation campaigns conducted in concert with cyber attacks on election infrastructure can amplify disruptions of electoral processes and public distrust of election results.

SCOPE NOTE: The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center (NRMC) prepared this risk assessment to support CISA efforts to help U.S. state and local governments mitigate vulnerabilities to election systems, and support cybersecurity and system resilience within election systems. This product provides base-level analysis election officials can use to prioritize and tailor risk management efforts to address specific vulnerabilities in high consequence election system components, and to promote cybersecurity and system resilience within election systems. Prioritizing mitigation of risk to potential cyber attacks on the integrity of election system components could yield the greatest marginal benefit in improving states' risk profiles.

CISA NRMC coordinated this analysis with the CISA Cybersecurity Division (CSD) and DHS's Office of Intelligence and Analysis (I&A) Cyber Mission Center (CYMC).

ELECTION INFRASTRUCTURE SYSTEMS OVERVIEW

Election infrastructure is comprised of a diverse set of systems, networks, and processes. The election system in the United States is not one system, but a collection of many different systems. Each jurisdiction's election infrastructure ecosystem is a collection of different components, some interconnected electronically and others not, that must function together to conduct elections. Although they perform the same functions, system processes and infrastructure vary from state-to-state and often differ even between counties, parishes, towns, or cities within a state or territory.[1]

Figure 1 provides a functional overview of a U.S. election ecosystem.

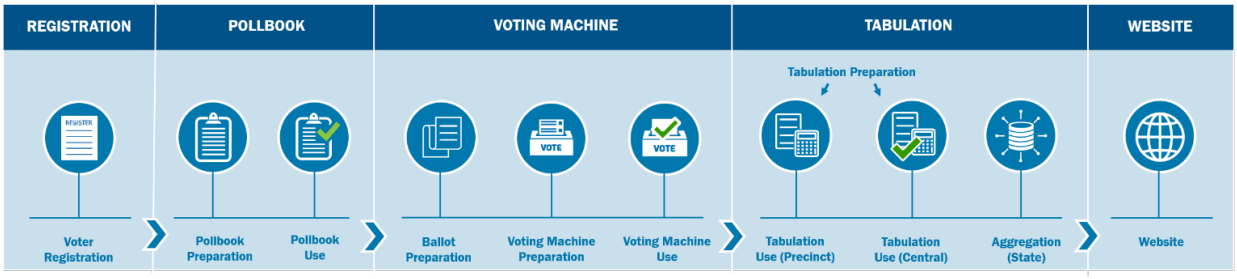


FIGURE 1—ELECTION SYSTEM FUNCTIONAL ECOSYSTEM

Election systems use diverse infrastructure and security controls. Even jurisdictions that deploy cybersecurity best practices are potentially vulnerable to attacks from sophisticated cyber actors, such as advanced nation-state actors. Therefore, detection and recovery methods are equally significant as preventative measures.

Cyber attacks on the integrity of state-level voter registration, pollbooks, and election websites, as well as on the preparation of ballots, voting machines, and tabulation systems, have the potential for greatest functional impact to the ability of jurisdictions to conduct elections, based on fault tree analysis[i] of election system components through each phase of the election process. The following election infrastructure represents the systems, networks, and processes most critical to the security, integrity, and resilience of U.S. elections:

- **Voter registration databases** are used to enter, store, and edit voter registration information, such as servers that host the database and online portals that provide access. Voter registration is an ongoing process to create new records, update existing records, and remove outdated records. Voter registration databases receive data automatically and indirectly (i.e. through manual entry) from a variety of sources, including other government agencies (e.g., the Department of Motor Vehicles) and organizations that aid in the registration process (e.g., voter registration campaigns). The databases contain information on whether people are entitled to vote, where they can vote, and on what unique ballot style they will vote, based upon voter geographical placement within multiple layers of political and taxing districts.
- **Electronic and paper pollbooks** contain information on registered voters at polling places, and can be used to register voters where permitted by law. Before use, pollbooks must be prepared by transferring information from the voter registration database. Pollbooks are comprised of both technology and processes to view, edit, and modify voter records. Pollbooks may be either networked or non-networked. Networked pollbooks are electronic pollbooks with a connection to an external

[i] Fault tree analysis is a widely used method in system reliability, maintainability, and safety analysis. It is a deductive procedure used to determine combinations of hardware and software failures and human errors that could cause undesired outcomes at the system level.

database, and may include a direct connection to the voter registration database or a separate server. Non-networked pollbooks are either paper pollbooks or static digital files on computers.

- **Ballot preparation** is the process of overlaying political geographies with the contests and candidates specific to each district, and then translating those layouts into unique combinations of ballot data. Ballot preparation data takes multiple forms such as ballot images (both paper and electronic), the data files necessary to build ballot images, audio files for special use ballots, and specific files for export to external systems such as websites or Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)-focused digital systems. Ballot preparation also generates the data necessary for tabulating votes within a voting machine, and aggregating tabulated votes within a jurisdiction or state. This process is usually completed in an election management system.
- **Voting machine systems** consist of the technology and processes used to cast and, in some cases, generate voter ballots of all types (paper-based systems, and electronic-based systems like ballot marking devices and direct-recording electronic machines with or without a voter-verified paper audit trail). Voting machines encompass both technology and processes used by election officials to prepare voting machines for ballot tabulation, and in some cases presentation. Specifically, this includes loading the ballot files created during ballot preparation onto voting machines. Voting machines are held in storage in the custody of election officials, but after delivery are placed at voting locations for use during early voting and on Election Day. Voting machines are the most visible form of technology that voters interact with during the voting process.
- Centralized **vote tabulation and aggregation systems** are used to tally votes shared by sub-jurisdictions such as counties, precincts, and in some cases individual machines or even individual ballots. These systems collect and process data to determine the result of an election contest. Tabulation encompasses both technology and processes used to count votes and aggregate results. Vote tabulation processes include hand counting, optical scans of paper ballots, and direct electronic tabulation. Vote tabulation may occur at the precinct-level in addition to centralized tabulation.
- **Official websites** are used by election officials to communicate information to the public, including how to register to vote, where to vote (e.g., precinct look-up tools), and to convey election results (e.g., election night reporting systems). Sometimes election websites are hosted on government-owned infrastructure, but are often hosted by commercial partners.
- **Storage facilities**, which may be located on public or private property, and may be used to store election and voting system infrastructure before Election Day.
- **Polling places** (including early voting locations) are locations where individuals cast their votes and may be physically located on public or private property.
- **Election offices** are locations where election officials conduct official business, including shared workspaces such as public libraries, municipal buildings, private homes, and public areas for jurisdictions without a dedicated workspace.

ELECTION INFRASTRUCTURE CYBER ATTACK CONSEQUENCES

Analysis determined that cyber attacks on each component of the election infrastructure ecosystem may have differing consequences, based on type of cyber impact and the specific targeted election system component. This assessment used the Confidentiality-Integrity-Availability (CIA) Triad information security model[ii] to analyze three types of cyber attacks:

- Confidentiality Attacks, the theft of information;
- Integrity Attacks, the changing of either the information within or the functionality of a system; and
- Availability Attacks, the disruption or denial of the use of the system.

[ii] (U) For more information on the CIA triad, refer to: Center for Internet Security, "EI-ISAC Cybersecurity Spotlight – CIA Triad," 2019, https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/. Accessed July 28, 2020.

Risks can also differ for the same component during preparation and during use (e.g., voting machines may be more accessible to cyber attacks during preparation than on Election Day). Additionally, a successful cyber attack on a voting machine could also cascade onto a tabulation or aggregation system if malware is transferred after voting is complete.

Table 1 provides a high-level overview of the potential consequence of a successful cyber attack by system component. This table does not directly address cyber attacks aimed at undermining public confidence in elections, though the three types of attacks could have a primary or secondary goal of undermining confidence.

TABLE 1—POTENTIAL CONSEQUENCE OF AN ELECTION CYBER ATTACK BY COMPONENT

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Voter Registration	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Pollbook Preparation	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Ballot Preparation	Expose Ballot Information	Change Ballot Information During Preparation	Prevent Ballot Preparation
Voting Machine Preparation	Change Voting Machine Functionality to Expose Voter Choices	Change Voting Machine Functionality (Presentation of Ballot/Recording of Choices)	Prevent Voting Machine Functionality
Tabulation Preparation	Change Tabulation Machine Functionality to Expose Results	Change Tabulation Machine Functionality	Prevent Tabulation Machine Functionality
Pollbook Use	Expose Non-public Voter Registration Information	Change Voter Registration Information (In Pollbook)	Prevent Access to Voter Registration Information
Voting Machine Use	Expose Voter Choices	Change Voting Machine Functionality	Prevent Voting Machine Functionality
Tabulation (Precinct)	Expose Tabulation Results Before Intended	Change Results of Vote Tabulation	Prevent Vote Tabulation
Tabulation (Central)	Expose Tabulation Results Before Intended (Aggregation)	Change Results of Vote Tabulation (Aggregation)	Prevent Vote Tabulation (Aggregation)
Aggregation (State)	Expose Aggregation Results Before Intended	Change Results of Vote Aggregation	Prevent Vote Aggregation
Website	Expose Information Not Intended for Public Disclosure	Change Reported Results	Prevent Reporting of Results

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Website	Expose Information Not Intended for Public Disclosure	Change Voter Registration and Precinct Information (In Voter Lookup)	Prevent Voter Lookup of Registration and Precinct Information

JOINT ELECTION INFRASTRUCTURE AND DISINFORMATION ATTACKS

Foreign state and non-state actors leverage information activities as part of broad campaigns to sow discord, manipulate public discourse, and discredit the electoral system to undermine pillars of democracy. In the context of elections, foreign entities aim to:

- Dissuade target audiences from participating in the electoral process through content that suggests their votes do not matter, that abstaining from voting is the most democratic action, or through content that misleads voters about the process of voting.
- Impact candidate selection through, among other activities, pushing fabricated and favorable content about preferred candidates, and fabricated or disparaging content about disfavored candidates.
- Damage the public perception of a fair and free election by pushing false or misleading content regarding election processes and results.

These disinformation campaigns, conducted in concert with cyber attacks on election infrastructure, can amplify disruptions of electoral processes and public distrust of election results. Unauthorized network access allows for surveillance and reconnaissance, and provides opportunities for destructive cyber attacks. Stolen or falsified information can be strategically leaked to shape false narratives. Hijacking online personas and the defacement or alteration of public-facing sites can be leveraged to influence public opinion. The targeting of government systems (even without compromise) can be used to form narratives leading to distrust of the government as stewards of citizen information.

ELECTION INFRASTRUCTURE RISK CRITERIA

Based on these consequences, the assessment applied multiple criteria that assess the scale of cyber risk associated with election infrastructure. The potential scale of an election infrastructure cyber attack is based on factors including whether the infrastructure is being prepared for use or is in use, whether infrastructure technology is networked, and the degree to which infrastructure components are centralized. Risk criteria considerations are not mutually exclusive.

CISA also assesses additional risk criteria related to voter registration, voting machines, and electronic submission of ballots.

Attack Scale: System Preparation

The potential scale of a cyber attack on election infrastructure will be more widespread if a cyber attack occurs during the preparation or programming of election infrastructure versus during its immediate use. While an integrity cyber attack on a single voting machine in a precinct would affect that machine or precinct, cyber attacks on a jurisdiction's central preparation or programming of machines may affect the entire jurisdiction using those machines. If preparation of machines is conducted at the state level, cyber attacks on the preparation process have the potential to impact an entire state. This is true for a single election. However, malware inserted into a single machine during use could propagate to the tabulation and preparations system,

and to all machines in future elections if jurisdictions do not follow best practices for using secure election software system builds.

During system preparation, election jurisdictions rely on files from external sources, such as registration databases, voting system vendors, ballot printers, or ballot programmers. Importing data from external sources raises risk, since sources may use internet connected systems that do not follow cybersecurity best practices. Additionally, an external source may present a cyber attack vector against a wide variety of election jurisdictions if a single source services multiple jurisdictions or states.

Attack Scale: System Networking

The scale of a cyber attack on election infrastructure has the potential to be more widespread if an attack compromises networked infrastructure. For example, electronic pollbooks in some jurisdictions are networked together across the jurisdiction to facilitate vote center operation, whereas electronic pollbooks in other jurisdictions are non-networked. A cyber attack on an individual non-networked pollbook has less chance to spread if the machine remains isolated from a network. An integrity attack on a networked e-pollbook has the potential to affect an entire jurisdiction, while an integrity attack on a local, non-networked pollbook can be isolated to that particular voting location.

Because of that, we assess network connectivity for voting systems to be high risk. Creating and maintaining an airgap for critical systems, such as the vote casting or vote tabulation systems, is a best practice.[iii]

Attack Scale: Centralization

The potential scale of a cyber attack will be more widespread if an attack targets a centralized process versus a localized process. Some jurisdictions tabulate votes at each polling location before aggregating results at a central location, while others only tabulate votes at a central location. An integrity attack on central tabulation systems or processes has the potential for a broader reach than an integrity attack on local tabulation process.

Table 2 provides a brief summary of criteria used to assess cyber risk associated with the potential scale of an election-related cyber attack, assessed by an election infrastructure component. We categorize the scale of an attack into one of three categories:

- Low: Affecting a subset of a jurisdiction
- Medium: Affecting an entire jurisdiction
- High: Affecting an entire state or multiple jurisdictions

For a more detailed look at cyber risk by component, refer to “Table 3—Election Infrastructure Risk Prioritization Matrix” on page 10.

[iii] An airgap is a physical separation between systems that requires data to be moved by some external, manual procedure.

TABLE 2—POTENTIAL SCALE OF AN ELECTION CYBER ATTACK BY COMPONENT

ELECTION COMPONENT	ATTACK VECTOR	SCALE
Voter Registration	Jurisdiction Registration Database	Medium
Voter Registration	State Registration Database	Heavy
Pollbook	Jurisdiction Pollbook Preparation	Medium
Pollbook	State Pollbook Preparation	Heavy
Pollbook	Non-Networked Pollbook Use	Low
Pollbook	Jurisdiction Networked Pollbook Use	Medium
Pollbook	State Networked Pollbook Use	Heavy
Ballot Preparation	Jurisdiction Ballot Preparation	Medium
Ballot Preparation	State Ballot Preparation	Heavy
Voting Machine	Jurisdiction Voting Machine Preparation	Medium
Voting Machine	State Voting Machine Preparation	Heavy
Voting Machine	Voting Machine Use	Low
Tabulation	Tabulation Preparation	Medium
Tabulation	Precinct Tabulation Use	Low
Tabulation	Central Tabulation Use	Medium
Tabulation	State Aggregation	Heavy

ELECTION COMPONENT	ATTACKER VECTOR	SCALE
Website	Jurisdiction Website	Medium
Website	State Website	Heavy

Number of Registered Voters

Electoral jurisdictions vary greatly in size, with some having as few as 100 voters to the largest encompassing several million voters.[2] Jurisdictions with more registered voters manage more risk than jurisdictions with smaller voter populations. The number of registered voters represents the number of individuals in each jurisdiction who could have personal information exposed during a confidentiality attack or experience disruptions at polling places as a result of cyber attacks, or election-related cascading impacts from physical incidents.

Voter Registration System Configuration

States manage their voter registration systems in three primary ways.[3] States with top-down voter registration system host data on a single, central platform of hardware, which is maintained by the state with data and information supplied by local jurisdictions. Bottom-up systems feature data hosted on local hardware and periodically compiled to form a statewide voter registration list. Hybrid systems are a combination of top-down and bottom-up characteristics. As of 2018, 39 states and territories have voter registration systems that are top-down configurations.[4]

States with top-down voter registration systems present attackers with a single system that, if compromised, could disrupt the voting process at a broader scale than jurisdiction-level systems. Since top-down voter registration systems maintain the entire voter registration database for a state, they present a single target for attack that could disrupt many more voters. A bottom-up or hybrid system would require the compromise of a diverse number of systems across a state to achieve similar results. However, cyber and physical security of top-down systems is more likely to be stronger than bottom-up or hybrid systems, based on a review of overall state and local cybersecurity resources and support.

Online Voter Registration

Online voter registration allows residents to complete voter registration forms online. Forty states and territories offer an online voter registration portal in which individuals can register on their own without having to submit a paper form.[5]

Online voter registration systems provide an additional point of vulnerability to enable cyber actors to gain access to voter registration databases and conduct confidentiality, integrity, or availability attacks.[6] Hackers, including nation-state actors, have exploited voter databases in the past to gain illicit access to voter information.[7]

Measures such as same day registration[iv] and provisional ballots are likely to reduce impact of integrity attacks to voter registration systems by providing a fail-safe mechanism to allow eligible voters to correct tampered or deleted data and vote using established processes. Help America Vote Act-required provisional ballot

[iv] Same day registration is the procedure for individuals to register to vote and cast a ballot on the same day. According to the U.S. Election Assistance Commission Election Administration and Voting Survey, 26 states have some form of same day registration, as of 2018.

processes[v] also provided a fail-safe measure of resilience. Even though same-day registration and provisional ballots can provide resiliency, both have the potential to cause disruptions at polling places due to longer processing times that can be required to administer provisional ballots (approximately 15 percent longer than that of normal ballot processes, depending upon the specific processes election officials deploy). Additionally, many election officials believe the best implementation of same-day registration utilizes network connected technology, such as electronic pollbooks, introducing system networking risks, as discussed above.

Voting Machines Without Voter Verified Auditable Paper Record

Direct-recording electronic voting machines capture voting data directly into electronic memory.[8] Many direct-recording electronic voting machines come equipped with a voter-verified paper audit trail feature that provides a printout, verifiable by voters, to ensure their votes are correctly captured. Since 2016, many election officials across the country replaced systems that do not have a voter verified auditable paper record with voting systems that do. Based on research, CISA estimates that greater than 90 percent of cast ballots in 2020 will have a corresponding auditable record.

We assess voting systems without a voter verified auditable paper record as presenting additional risk, based on analysis of the difficulty of identifying electronic manipulation to ensure election integrity in the event of a cyber attack. The existence of a voter verified auditable paper record is the first step in building resiliency, as it can provide the ability for election officials to verify that the outcomes of the election are correct regardless of whether an undetected error or fault in the voting system occurs. However, to provide voters high assurance that errors will be detected, election officials must also conduct regular audits of their elections.

Logic and accuracy testing measures such as parallel monitoring[vi] and hash checks[vii] to ensure software integrity against certified software builds are likely to improve the detection and recovery capability of election officials with regard to their voting systems; especially those without a record that cannot be otherwise audited, though neither measure can replace the use of paper backups to identify irregularities and reduce risk.

Uniformed and Overseas Citizens Absentee Voting Act Electronic Ballots

Certain groups of voters, particularly military and overseas voters, face challenges voting both in-person or through the mail. All jurisdictions are required to offer electronic ballot delivery, per federal law. Many state and local election officials additionally make use of email, fax, and web portals to aid in ballot return for these groups.[9,10] Thirty-one states[viii] and the District of Columbia (D.C.) allow voters covered by the Uniformed and Overseas Citizens Absentee Voting Act to submit their ballots by at least one electronic means, such as internet portal, email, or fax.[11] Five states (Arizona, Colorado, Missouri, North Dakota, and West Virginia) allow Uniformed and Overseas Citizens Absentee Voting Act voters to return ballots using a web-based portal or application. Additionally, several counties within Utah, Colorado, and Oregon conducted a pilot using a mobile voting application and are determining its use moving forward.[12] West Virginia used a similar application in previous elections. Nineteen states[ix] and D.C. allow some voters to return ballots via email or fax, while seven states[x] allow some voters to return ballots via only fax.

---

[v] Provisional ballot processes, or provisional voting, maintains the individual's intent to vote until election officials determine the eligibility status of the individual to cast a ballot in the election. All states except for Minnesota, New Hampshire, and North Dakota issue provisional ballots to individuals on election day, per Section 302 of the Help America Vote Act.

[vi] Parallel monitoring is the process of testing a set of randomly selected voting machines to be tested in election mode during the voting period. The intent is to try to "trick" the system into thinking that it is in a voting location and being used live in the election. Parallel testing could then detect if malicious software had been deployed to only take effect in a specific mode (i.e. Election Mode) or during a specified time (i.e. on Election Day).

[vii] Hash checks are useful to verify data integrity and are conducted by comparing the hash value of received data to the hash value of data as it was sent to detect whether data was altered.

[viii] The 31 states are: Alaska, Arizona, California, Colorado, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Texas, Utah, Washington, and West Virginia.

[ix] The 19 states are: Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oregon, South Carolina, Utah, and Washington.

[x] The seven states are: Alaska, California, Florida, Louisiana, Oklahoma, Rhode Island and Texas.

We assess electronic ballot return as presenting additional risk, whether through email, fax, web portal, or mobile application, based on the difficulty of securing the electronic transmission of data. Ballots submitted through electronic means are subject to increased potential to disruption, manipulation, or exposure.

Risks to electronic ballot return are similar to mail-in ballots, but with the potential to impact a higher number of ballots. For example, a man-in-the-middle attack on a physical mail-in ballot requires physical access, and attack scale is limited through proper chain of custody procedures. In contrast, a malicious cyber actor can conduct a man-in-the-middle attack on electronic ballots at a higher scale from a wide range of global locations.

ELECTION INFRASTRUCTURE RISK PRIORITIZATION MATRIX

CISA NRMC assesses differing relative aggregate cyber risk per election infrastructure component, based on fault tree analysis. The prioritization matrix below is calculated based on the technical capability required to conduct a cyber attack,[xi] the potential scale of impact of a cyber attack, and an importance score[xii] to provide a view of risk across election system components. Since election system implementations vary widely among jurisdictions, CISA NRMC evaluated both a "best-case" and "worst-case" system implementation for each election component. This view of "best-case" and "worst-case" impacts the technical capability required to attack each component, but does not alter the attack scale or importance.

Table 3 provides a detailed look at the relative cyber risk to election components in best case (most secure) and worst case (most vulnerable) system implementation, assessed by component and cyber attack type. The table represents the change in risk rating when implementing recommended security controls rather than low security controls. For election infrastructure systems implementing low levels of security controls, we assess nearly any capable threat actor may possess the ability to conduct successful attacks on election infrastructure systems. In contrast, implementing recommended security controls on election infrastructure significantly lowers risk of a successful cyber attack. Some components, even with recommended security controls implemented, represent higher risk to availability attacks as detailed in the below table.

TABLE 3—ELECTION INFRASTRUCTURE RISK PRIORITIZATION MATRIX

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Jurisdiction Registration Database	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Registration Database	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Registration Database	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low

[xi] The technical capability was determined based on the relative difficulty of an attack on the component.
[xii] The importance score was determined based on aggregate importance scale measures assigned by an expert group of elections officials and technology providers.

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
State Registration Database	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Registration Database	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Registration Database	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium
Jurisdiction Pollbook Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Pollbook Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Pollbook Preparation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Medium
State Pollbook Preparation	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Non-Networked Pollbook Use	Confidentiality	Low	Tier 3 Actor	Low	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Non-Networked Pollbook Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Non-Networked Pollbook Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Jurisdiction Networked Pollbook Use	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Networked Pollbook Use	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Networked Pollbook Use	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Networked Pollbook Use	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Networked Pollbook Use	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Networked Pollbook Use	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Jurisdiction Pollbook Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Pollbook Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Jurisdiction Pollbook Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Ballot Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Ballot Preparation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Ballot Preparation	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium
Jurisdiction Voting Machine Preparation	Confidentiality	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Voting Machine Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Voting Machine Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Voting Machine Preparation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Voting Machine Preparation	Integrity	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Voting Machine Preparation	Availability	High	Tier 3 Actor	Heavy	Tier 2 Actor	Medium

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Voting Machine Use	Confidentiality	Low	Tier 3 Actor	Heavy	Tier 1 Actor	Low
Voting Machine Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Voting Machine Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Tabulation Preparation	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Tabulation Preparation	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Tabulation Preparation	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
Precinct Tabulation Use	Confidentiality	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Precinct Tabulation Use	Integrity	Low	Tier 3 Actor	Low	Tier 1 Actor	Low
Precinct Tabulation Use	Availability	Low	Tier 3 Actor	Low	Tier 2 Actor	Low
Central Tabulation Use	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Central Tabulation Use	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low

COMPONENT	ATTACK TYPE	ATTACK SCALE	*LOW CONTROLS* ATTACKER SKILL	*LOW CONTROLS* RISK RATING	*RECOMMENDED CONTROLS* ATTACKER SKILL	*RECOMMENDED CONTROLS* RISK RATING
Central Tabulation Use	Availability	Medium	Tier 3 Actor	Medium	Tier 2 Actor	Low
State Aggregation	Confidentiality	High	Tier 3 Actor	Medium	Tier 1 Actor	Low
State Aggregation	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Aggregation	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Medium
Jurisdiction Website	Confidentiality	Medium	Tier 3 Actor	Low	Tier 1 Actor	Low
Jurisdiction Website	Integrity	Medium	Tier 3 Actor	Medium	Tier 1 Actor	Low
Jurisdiction Website	Availability	Medium	Tier 3 Actor	Low	Tier 2 Actor	Low
State Website	Confidentiality	High	Tier 3 Actor	Low	Tier 1 Actor	Low
State Website	Integrity	High	Tier 3 Actor	Heavy	Tier 1 Actor	Low
State Website	Availability	High	Tier 3 Actor	Medium	Tier 2 Actor	Low

ATTACK TYPE
***Confidentiality*: the theft of information**
***Integrity*: the changing of either the information within or the functionality of a system**
***Availability*: the disruption or denial of the use of the system**

ATTACK SCALE
***Low*: Affecting a subset of a jurisdiction**
***Medium:* Affecting an entire jurisdiction**
***High:* Affecting an entire state or multiple jurisdictions**

ATTACKER SKILL- LOW/RECOMMENDED CONTROLS
Each capability score was determined based on the relative difficulty of an attack on the component for worst case and best case implementation of system security controls and indicates the technical capability needed by a threat actor to execute a potentially successful attack.

***Tier 1 Actor*: Most capable threat actors that can discover new vulnerabilities ("zero days"), develop custom exploits and tools, and combine online activities with close physical operations. Tier 1 actors include both nation-state and sophisticated sub-national groups.**

***Tier 2 Actor*: Moderately capable threat actors that can exploit most cyber vulnerabilities with sufficient time and can create custom exploits and tools. Tier 2 actors are largely limited to conducting operations over the Internet, through they can also exploit proximate access (e.g., "wardriving") or lax security policies on removable media.**

***Tier 3 Actor*: Lease sophisticated threat actors that rely on readily-available cyber tools to exploit known vulnerabilities. Tier 3 actors do not create their own exploits or tools, but can find them on the dark-web or in existing tool suites.**

RISK RATING- LOW/RECOMMENDED CONTROLS
Each overall risk rating score was determined for both the worst case and best case implementation of system security controls. Ratings are based on aggregate cyber capability and attach scale measures and assessments by an expert group of elections officials and technology providers.

---

[1] RAND Corporation Homeland Security Operational Analysis Center, "Election System Risk Prioritization Report," August 2019, page 1.
[2] David C. Kimball and Brady Baybeck, "Are All Jurisdictions Equal? Size Disparity in Election Administration," Election Law Journal (Vol. 12, No. 2), 2013, pp.130-145.
[3] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 119.
[4] Ibid.
[5] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 122.
[6] National Conference of State Legislatures, "Online Voter Registration," October 25, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx. Accessed July 28, 2020.
[7] Report of the U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure,* page 22.
[8] Verified Voting Foundation, "Voting Equipment in the United States," 2019, https://www.verifiedvoting.org/resources/voting-equipment/. Accessed July 28, 2020.
[9] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 15.
[10] National Conference of State Legislatures, "Electronic Transmission of Ballots," September 5, 2019. https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed July 28, 2020.
[11] Ibid.
[12] Associated Press, "2 Oregon counties offer vote-by-mobile to overseas voters," 2019, https://apnews.com/8ce0fbc400514f55839fa84fb364d7f4. Accessed July 28, 2020.

The Cybersecurity and Infrastructure Security Agency (CISA), National Risk Management Center (NRMC), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. For more information, contact Central@cisa.gov or visit https://www.cisa.gov/national-risk-management.

PDM 20004

EXHIBIT 7

TOUHY **STATEMENT**

Pursuant to 6 C.F.R. § 5.45(a), the nature and relevance of the information sought by the foregoing subpoena ("Subpoena") are as follows.

The parties on behalf of whom the Subpoena was issued, My Pillow, Inc. and Michael Lindell, are defendants in *Smartmatic USA Corp. et al. v. Lindell et al.*, no. 22-cv-0098-WMW-JFD in the United States District Court for the District of Minnesota ("the Action"). Plaintiffs in the Action are three entities (collectively "Smartmatic") who market electronic equipment and software used to cast ballots and perform other election administration tasks. Smartmatic alleges that Michael Lindell, the chief executive officer of My Pillow, Inc., defamed it by making statements about the 2020 presidential election, and that My Pillow, Inc. bears legal responsibility for Mr. Lindell's statements. The allegedly defamatory statements by Mr. Lindell state in part that Smartmatic's equipment was manipulated by unauthorized persons, including foreign actors, to change votes in the 2020 election; that algorithms within Smartmatic equipment changed votes; and that Smartmatic equipment was hacked to affect election results.

Defenses to Smartmatic's defamation claims include that Mr. Lindell did not speak with "actual malice," under the doctrine of *New York Times v. Sullivan*, and therefore his statements are protected by the First Amendment, or that Mr. Lindell's statements were substantively true. One of the considerations relevant to "actual malice" is the plausibility of the statements that were made. Defendants are entitled to obtain discovery of facts, in a form admissible in a federal court, that would tend to support or weaken these defenses. The information sought by the Subpoena is relevant to these considerations.

Topic 1 is relevant and important to the claims and defenses in the Action because the Smartmatic plaintiffs, in their operative complaint, cite and rely upon the November 12, 2020 Joint Statement by CISA and other government entities for the proposition that there was no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised in the 2020 presidential election. The Smartmatic plaintiffs said that Lindell should have accepted the representations made in the Joint Statement as correct. The Defendants accordingly seek to ascertain the factual basis of the Joint

Statement, and the process used to produce the Joint Statement, to counter Smartmatic's arguments based upon the Joint Statement.

Topic 2 is relevant and important to the claims and defenses in the Action because in 2022 CISA published an advisory identifying specific vulnerabilities in certain voting equipment, which could permit the alteration of votes. Defendants seek to discover any information known by CISA concerning the potential exploitation of these vulnerabilities. Such information, depending on its substance, would support both the plausibility and the truthfulness of the allegedly defamatory statements at issue in the Action.

Topics 3 and 4 are relevant and important to to the claims and defenses in the Action because the occurrence of unauthorized access to electronic voting systems in the United States would support both the plausibility and the truthfulness of the allegedly defamatory statements at issue in the Action.

Topic 5 is relevant and important to the claims and defenses in the Action because one argument raised against the allegedly defamatory statements at issue is the assertion that election equipment was not connected to the Internet during the 2020 election. Knowledge by CISA to the contrary would support both the plausibility and the truthfulness of the allegedly defamatory statements at issue in the Action.

Topic 6 is relevant and important to the claims and defenses in the Action because Defendants previously issued a document subpoena to CISA seeking information concerning these topics, and CISA's response indicated that CISA did not have any documents responsive to certain requests. The absence of documentation responsive to these requests supports Defendants' anticipated arguments that the Joint Statement was not a document that Lindell was obligated to accept at face value. Defendants need to obtain, in admissible form, evidence of the absence of the referenced documentation, and the meaning of that absence (based on the scope of CISA's search for responsive documents).

Topic 7 is relevant and important to the claims and defenses in the Action because it shows that CISA, a source relied upon by the Smartmatic plaintiffs, identifies the threat of incidents like the substance of the allegedly defamatory statements at issue in the Action are genuine threats to election security.

Topic 8 is relevant and important to the claims and defenses in the Action because it shows that CISA, a source relied upon by the Smartmatic plaintiffs, prior to the 2020 election about which the allegedly defamatory statements at issue in the Action were

made, publicly identified risks to election security that match the substance of the allegedly defamatory statements at issue in the Action.

Compliance with the deposition Subpoena would not be unduly burdensome or otherwise inappropriate, because providing testimonial evidence related to these matters about which CISA has publicly spoken should be well within the existing knowledge of CISA. To respond to the Subpoena, CISA need merely marshal the knowledge already held by it, and well documented, to provide the fuller context of public statements CISA has already made.

No privilege precludes disclosure of the factual information sought by the deposition Subpoena.

The public interest strongly favors transparency concerning these matters of great public concern, which have occupied the attention of large numbers of Americans since the 2020 election. In addition, the amount of damages claimed by Smartmatic in the operative complaint is in excess of $1 billion. The public interest favors providing relevant facts to assist in the fair and accurate determination of an action of such magnitude. Shrouding information developed and held by the people's government from them has negative effects on public confidence concerning elections.

While providing a deposition would require some time and effort from CISA, the relative burden is low. Moreover, providing information regarding these matters is part of the official business of CISA. This is not a deposition subpoena asking the agency to go outside of the subject matter that is the basis for its existence; it is a request that the agency provide information about matters at the core of its mission.

The requested information does not implicate any concerns about impartiality between private litigants. On the contrary, a deposition would advance the cause of impartiality. The Smartmatic plaintiffs already enjoy information and communication with federal cybersecurity officials as a result of their business activities. Providing the Defendants with a window into the same would balance the playing field in some measure, not unfairly tilt it.

EXHIBIT 8

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S NOTICE OF SERVING SUBPOENA FOR VIDEOTAPED DEPOSITION OF ANDREW APPEL**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Andrew Appel, 43 Philip Drive, Princeton, NJ 08540. A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 19, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 19, 2023 a true and accurate copy of the foregoing was served via email to the following attorneys of record for Plaintiffs:

ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402

Christopher K. Larus	CLarus@robinskaplan.com
William E. Manske	WManske@robinskaplan.com
Emily J. Tremblay	ETremblay@robinskaplan.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

J. Erik Connolly	EConnolly@beneschlaw.com
Nicole E. Wrigley	NWrigley@beneschlaw.com
Michael E. Bloom	MBloom@beneschlaw.com
Laura A. Seferian	LSeferian@beneschlaw.com
Julie M. Loftus	JLoftus@beneschlaw.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
200 Public Square, Suite 2300
Cleveland, OH 44114

Alyssa A. Moscarino	AMoscarino@beneschlaw.com
James R. Bedell	JBedell@beneschlaw.com

DATED: September 19, 2023 By: *Andrew D. Parker*

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al.
Plaintiff
v.
Michael J. Lindell and My Pillow, Inc., et. al.
Defendant

Civil Action No. 21-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Andrew Appel
43 Philip Drive, Princeton NJ 08540
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about t these matters: **See, attached Exhibit A.**

Place:	Date and Time:
Veritext Office Suites 290 W Mount Pleasant Avenue Suite 3200 Livingston , NJ, 07039	October 16, 2023 at 9:00 a.m. EDT

The deposition will be recorded by this method: stenographic and videotaped

❒ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 09/19/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

s/ Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* **Defendants' Michael J. Lindell and My Pillow, Inc., et al.**, who issues or requests this subpoena, are:

Andrew Parker, 123 N. 3rd Street, Suite 888, Minneapolis MN 55401, parker@parkerdk.com, 612-355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 21-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____ _____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S AMENDED NOTICE OF SERVING SUBPOENA FOR VIDEOTAPED DEPOSITION OF THOMAS MCINERNEY**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Thomas McInerney, 12155 Sangsters Court, Clifton VA 20124. A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 19, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 19, 2023 a true and accurate copy of the foregoing was served via email to the following attorneys of record for Plaintiffs:

ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402

Christopher K. Larus	CLarus@robinskaplan.com
William E. Manske	WManske@robinskaplan.com
Emily J. Tremblay	ETremblay@robinskaplan.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

J. Erik Connolly	EConnolly@beneschlaw.com
Nicole E. Wrigley	NWrigley@beneschlaw.com
Michael E. Bloom	MBloom@beneschlaw.com
Laura A. Seferian	LSeferian@beneschlaw.com
Julie M. Loftus	JLoftus@beneschlaw.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
200 Public Square, Suite 2300
Cleveland, OH 44114

Alyssa A. Moscarino	AMoscarino@beneschlaw.com
James R. Bedell	JBedell@beneschlaw.com

DATED: September 19, 2023 By: *Andrew D. Parker*

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al.
Plaintiff
v.
Michael J. Lindell and My Pillow, Inc., et. al.
Defendant

Civil Action No. 21-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Thomas McInerney
12155 Sangsters Court, Clifton VA 20124
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about t these matters: **See, attached Exhibit A.**

Place:	Date and Time:
Kingstone Ridge 5680 King Centre Drive, Suite 600 Alexandria, VA 22315	October 16, 2023 at 9:00 a.m. EDT

The deposition will be recorded by this method: stenographic and videotaped

❒ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 09/19/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

s/ Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* **Defendants' Michael J. Lindell and My Pillow, Inc., et al.**, who issues or requests this subpoena, are:

Andrew Parker, 123 N. 3rd Street, Suite 888, Minneapolis MN 55401, parker@parkerdk.com, 612-355-4100

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 21-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____ on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD **DEFENDANT'S AMENDED NOTICE OF SERVING SUBPOENA FOR VIDEOTAPED DEPOSITION OF ALAN DUKE**

TO: PLAINTIFFS ABOVE NAMED AND THEIR COUNSEL OF RECORD

PLEASE TAKE NOTICE that Defendants My Pillow, Inc. and Michael Lindell intend to serve a subpoena for deposition, pursuant to Fed. R. Civ. P. 45, upon Alan Duke, 4949 Genesta Ave Unit 105, Encino CA 91316. A copy of the subpoena and associated exhibits are attached hereto.

DATED: September 19, 2023

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (#195042)
Joseph A. Pull (#0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
123 N. Third Street, Suite 888
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 19, 2023 a true and accurate copy of the foregoing was served via email to the following attorneys of record for Plaintiffs:

ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402

Christopher K. Larus	CLarus@robinskaplan.com
William E. Manske	WManske@robinskaplan.com
Emily J. Tremblay	ETremblay@robinskaplan.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606

J. Erik Connolly	EConnolly@beneschlaw.com
Nicole E. Wrigley	NWrigley@beneschlaw.com
Michael E. Bloom	MBloom@beneschlaw.com
Laura A. Seferian	LSeferian@beneschlaw.com
Julie M. Loftus	JLoftus@beneschlaw.com

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP
200 Public Square, Suite 2300
Cleveland, OH 44114

Alyssa A. Moscarino	AMoscarino@beneschlaw.com
James R. Bedell	JBedell@beneschlaw.com

DATED: September 19, 2023 By: *Andrew D. Parker*

AO 88A (Rev. 12/20) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

Smartmatic USA Corp., et al. *Plaintiff* v. Michael J. Lindell and My Pillow, Inc. *Defendant*	)	Civil Action No. 21-cv-0098-WMW-JFD

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Alan Roderick Duke
4949 Genesta Ave Unit 105, Encino CA 91316
(Name of person to whom this subpoena is directed)

☑ Testimony: YOU ARE COMMANDED to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must promptly confer in good faith with the party serving this subpoena about the following matters, or those set forth in an attachment, and you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about these matters: See attached Exhibit A

Place:	Date and Time:
Veritext Conf. Suite 2049 Century Park E Suite 2480, Century City , CA, 90067	October 18, 2023 at 9:00 am PDT

The deposition will be recorded by this method: stenograph and videograph

❒ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 09/19/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

Andrew D. Parker
Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Defendants Michael J. Lindell and My Pillow, Inc., who issues or requests this subpoena, are:

Andrew Parker, 123 N. 3rd St, Suite 888, Minneapolis MN 55401; (612) 355-4100, parker@parkerdk.com

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 21-cv-0098-WMW-JFD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____ on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named individual as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY PILLOW, INC.,

Defendants.

Case No. 22-cv-00098- WMW-JFD

PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION

The Court enters the following Protective Order in this case,

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited (collectively, "Smartmatic") and Defendants Michael J. Lindell and My Pillow, Inc., (collectively, "Defendants"; Smartmatic and Defendants are collectively the "Parties") are engaged in discovery proceedings, which include, among other things, taking depositions, answering interrogatories, and producing documents. The Parties believe that certain information they have produced or will produce may contain information that is proprietary, commercially sensitive, or non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the "Order") will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to requests for admission, and responses to requests for documents, and any other information or

material produced, given, or exchanged, including any information contained therein or derived therefrom ("Discovery Material"), by or among any Party or non-Party providing Discovery Material (each a "Producing Party") in the above-captioned action (the "Litigation") to the party receiving the Discovery Material ("Receiving Party").

1. Any Producing Party may designate any Discovery Material as "Confidential Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party's or non-party's business or the business of any of that Party's or non-party's customers or clients.

2. Any Producing Party may designate any Discovery Material as "Attorneys' Eyes Only Discovery Material" under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys' Eyes Only Discovery Material. Attorneys' Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. Any Confidential Discovery Material and Attorneys' Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party, solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in

this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).

b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or (ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or

Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5.

After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in part only to the following persons for use in connection with the Litigation and in accordance with this Order:

a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;

b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;

c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;

d. Persons who appear as an author or recipient on the face of the document to be disclosed;

e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;

g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain

confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;

h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or

i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not a current or former employee of Smartmatic or Defendants subject to a non-disclosure agreement, (ii) is not a current competitor of Smartmatic or Defendants, an employee of a current competitor of Smartmatic or Defendants, or advising or discussing

employment with, or a consultant to, a current competitor of Smartmatic or Defendants, (iii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iv) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be

bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with Local Rule 5.6.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within

fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties have the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;

b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or

contains or reflects trade secrets or any other type of confidential information;

c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;

d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;

e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or

g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by

a Producing Party or Parties, such inadvertent production will in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.

b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging

privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only

Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of

Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The production of any Discovery Material by any non-party is subject to and governed by the terms of this Order.

28. If a Party violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. The Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any violation thereof.

Dated: November 3, 2022

s/ John F. Docherty
JOHN F. DOCHERTY
United States Magistrate Judge

EXHIBIT A

Smartmatic USA Corp., et al., v. Lindell, et al., Case No. 22-cv-0098-WMW-JFD

I have read the Protective Order Dated _____, 2022 in this action (the "Order") and undertake to access and use Discovery Material, Confidential Material, and Attorneys' Eyes Only Material only as the Order permits.

Signed this ___ day of _____, 2022.

_____
[Name]